



MIDWEST RELIABILITY MATTERS

JANUARY 2011

Special points of interest:

- Example of a “Good Self Report” (pg. 3)
- Demonstrating compliance with CIP Standards (pg. 5)
- MRO releases Case Notes (pg. 5)

Inside this issue:

- From the President **1**
- TIPS and Lessons Learned **3**
- Operations Update **6**
- Standards Update **7**
- Finance Update **7**
- Compliance Update **8**
- Industry Updates **15**
- Contacts and Calendar **16**

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**

A Bump in the Night

MRO President, Daniel P. Skaar

Is a “Bump in the Night” Inevitable? NO!

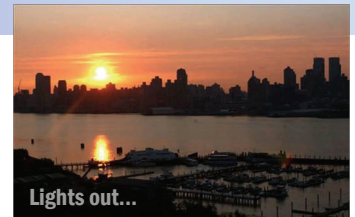
A case for cultures that embrace Reliability through the ERO-Model

This Scottish Prayer dates back at least to the early 1900s.

*From goulies and ghosties and
long-leggedy beasties
And things that go bump in the night
Good Lord, deliver us!*

Here at Midwest Reliability Organization, we say:

*From vegetation and misoperations and
poor communications
And things that go bump in the night
Good cultures of reliability, deliver us!*



The recent financial crisis, coupled with the oil debacle in the gulf, have undermined public confidence in regulatory models that bring government and the private sector together in a partnership. The current Electric Reliability Organization (ERO) model to ensure the reliability of the bulk power system is in its infancy and certainly has been under stress. Commentators have noted that FERC’s March 18 Orders¹, “portend a significant expansion of Federal Energy Regulatory Commission (FERC) control over the development and drafting of mandatory Reliability Standards by the North American Electric Reliability Corporation (NERC).” While MRO staff has no position with regard to these comments, we understand the concern.

The ERO model evolved from voluntary “self regulation” due to reaction to the 2003 Blackout. Our current “delegated authority model,” where the government delegates authority to qualified non-government organizations to carry out activities authorized under law, retains certain key aspects of “self regulation.” Key aspects include stakeholder participation in the standards setting process, the conduct of bulk system assessments, and representation at a regional level through MRO’s balanced shareholder board and on a North American-wide level through NERC (as the ERO) for industry-wide matters. It’s a private-public partnership which recognizes the interdependencies that link us together in the common goal of preventing cascading outages like the 2003 Blackout...keeping the lights on. Even further, we need to keep in mind that one of the greatest trading and security relationships in the world is the one between the United States and Canada. The ERO model recognizes these interdependencies and the need for continent-wide standards to assure trade is efficient and the security of our citizens is protected through close cooperation. The bulk electric system is the life blood to our economies and is essential to the well being of our citizens.

MRO staff continues to believe that the current international ERO model, established by the U.S. Congress with the cooperation and participation of Canada and Mexico, can ensure reliability and resiliency of the bulk power system with an emphasis on industry participation, and is a forward thinking, effective model that can detect, control and minimize risk to bulk power system reliability. (We are only three years into this model, and the next three years are pivotal as we must work out the “kinks” and maintain laser focus on evaluating and addressing risks to reliability - the essential purpose and the true value of the ERO model.)

The alternative to the current model is “strict” regulation where government makes and enforces all of the rules. Experts believe that an approach where the government exercises full monopoly power on making and enforcing the rules will be less effective due to the potentially diminished role of

¹ <http://ferc.morganlewis.com/2010/06/14/ferc-denies-rehearing-on-tpl-002-0-reliability-standard/>

(Continued from page 1--From the President)

stakeholders and their technical expertise². MRO staff is very mindful that leveraging the collective knowledge of the industry is a necessity for success in reliability regulation because of the complexity of the system and the underlying interdependencies of grid operators. Therefore, no matter what we call the regulation, it must find ways to work alongside the industry with effective “arms length” oversight, including policies and actions which are both proportionate and risk-based.

MRO staff believes that industry stakeholders should support the ERO model by assuring that the industry and NERC are focused on “prevention of systemic failure”³ and committed to “the broader public interests and policy goals”⁴ of reliability and public safety⁵.

Professor Andrew King⁶ notes the following important characteristics of self-regulatory models which we believe are applicable to our ERO model and really, any effective regulatory model:

- Impartial and independent third party evaluation of compliance
- Effective sanctioning
- Sophisticated stakeholders, and
- Effective processes for “discussion, negotiation, and the creation of new rules”

MRO staff would add one more characteristic at the beginning of the list, and that is: *those in the industry must embrace a culture of reliability, with compliance as a key element that provides assurance that reliability goals (including standards), are being met.*

A culture of reliability begins with the board of directors and the CEO. Dr. Zack T. Pate⁷ addressing nuclear safety stated: “An organization is strongly influenced by and is very responsive to perceived expectations from the top. And these perceived expectations can and often do have a profound impact on the behavior of the individuals in the organization.” If the “tone at the top” includes “reliability,” then compliance will be a key instrument of reliability. And, compliance is not just about reliability standards. It should include procedures that are considered best practices that address reliability which may not be embodied in a reliability standard at this time. Further, MRO staff believes that compliance provides a level of assurance that those in the industry are meeting reliability standards and those procedures which drive reliable bulk power systems. More on that later...

In the beginning

The cascading events of the Blackout of 2003 resulted from poor vegetation management, misoperations of relay and protection systems, and incomplete communications be-

tween grid operators coupled with inadequate training. The Energy Policy Act of 2005 responded by making reliability standards mandatory, granting significant penalty authority to the government of up to \$1 million per day in the U.S. For most Registered Entities (those Entities on the MRO registry), the first step in responding to mandatory reliability standards was to ensure compliance with those standards and minimize the risk of significant penalties. A key MRO priority was to make sure we had the processes in place for effective compliance monitoring and enforcement of violations, and address matters unique to Manitoba and Saskatchewan jurisdictions.

Where we are now

Some of the elements of an effective ERO model are well developed and others continue to improve. MRO staff believes that we do have an impartial, independent evaluation of compliance and that enforcement determinations are conducted without discrimination. Additionally, stakeholders in the MRO Region are sophisticated, and many are highly engaged in reliability policy matters. MRO staff has seen substantial improvements made to Registered Entity systems and compliance programs, and, working jointly with stakeholders, MRO has tracked numerous recommendations from the analysis of events that occurred on the bulk power system.

That said, there is room for improvement in the implementation of the ERO model. While standards (and the process for developing standards) are being addressed by the ERO, MRO staff believes that messages through enforcement must be consistent with establishing strong reliability. It’s simply following the matching principle: risks and materiality need to match investments and costs. The result is more effective sanctioning. Additionally, effective analysis of system events provides “low hanging” fruit for improvements to reliability and is an important component of a culture of reliability. To that end, MRO staff has been active in the following key areas.

First, Sara Patrick, Director of Enforcement and Regulatory Affairs, is leading an effort to scale enforcement proceedings with the seriousness of the violation. For example, minor violations should be dealt with in a routine, less formalized, and most importantly, *less costly* manner. The initial efforts have resulted in an administrative citation for minor violations. Hopefully this will free up resources for more important reliability matters.

Second, as MRO President, I recently filed comments in connection with the presentation I gave at the FERC Technical Conference on Reliability Monitoring, Enforcement and Compliance Issues held on November 18, 2010 [Docket No. AD11-1-000]. My comments included two specific suggestions to improve effective sanctioning.⁸

- 1) Develop a method of “scoring and recording” lesser

(Continued on page 13)

If the “tone at the top” includes “reliability,” then compliance will be an instrument of reliability.

² Omarova, Saule T., Rethinking the Future of Self-Regulation in the Financial Industry (October 20, 2010). Brooklyn Journal of International Law, Vol. 35, No. 3, p. 665, 2010 at footnote 21; UNC Legal Studies Research Paper No. 1695031. Available at SSRN: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1695031

³ *Id.*, at page 670.

⁴ *Id.*

⁵ Reference to May 29, 2009 remarks by President Obama regarding “Security of our Nation’s Infrastructure” <http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure>

⁶ Professor of Business Administration, Tuck School of Business at Dartmouth. See The Promise and Peril of Industry Self Regulation <http://www.tuck.dartmouth.edu/news/articles/the-promise-and-peril-of-industry-self-regulation> and Self Regulation vs. Risky Business <http://www.tuck.dartmouth.edu/news/articles/self-regulation-vs-risky-business/>

⁷ See PowerPoint presentation by Jim Ellis at http://www.hss.doe.gov/healthsafety/ism/SafetyCulture/OperatorsPerspective_JimEllis_05.pdf. Slide 19.

⁸ MRO President, Daniel P. Skaar, [remarks](#) on FERC November 18 Technical Conference



TIPS and Lessons Learned

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.

What Makes a “Good” Self Report?

Maximizing Self Report Credit in an MRO Enforcement Action

Since June 18, 2007, when the NERC Reliability Standards became mandatory and enforceable, the largest percentage of possible violations have been the result of Registered Entities self reporting potential non-compliance with Reliability Standards. The practice of self reporting and the fact that this discovery method represents the largest percent of possible violations are key to the success of the self-regulatory model in which the Compliance Monitoring and Enforcement Program was developed. The NERC Sanction Guidelines direct the Regions to consider whether a possible violation was self reported and whether the Registered Entity voluntarily undertook corrective action. In its “Policy Statement on Compliance” issued October 16, 2008, the Federal Energy Regulatory Commission (FERC) emphasized the “prompt detection, cessation, and reporting of the offense” as a key factor in establishing an effective compliance program. Beyond the NERC Sanction Guidelines and FERC’s Policy Statement, many regulators across the globe point to these same qualities—they truly are universal.

Over the course of time, MRO has seen remarkable improvement in the quality of the Self Reports being submitted. This is a testament to the industry gaining an understanding of the Reliability Standards and taking seriously the obligation of “prompt detection, cessation, and reporting” as essential to an effective compliance program. A quality Self Report consists not only of identifying the Reliability Standard and Requirement at issue, but also giving enough description to allow MRO to understand the nature, cause and duration of the possible violation. Ideally, the Self Report will include dates of possible noncompliance, a description of how the possible noncompliance was identified and what caused the possible violation, as well as any corrective actions (if any) that were taken upon identification, and what future corrective actions may be planned.

Additionally, in evaluating a Self Report, MRO will consider:

- Did the Registered Entity timely self report when it discovered or learned of the possible violation?
- Did senior management actively participate and encourage employees to provide complete information?
- Did the Registered Entity take immediate steps to address the possible violation and did these steps effectively create adequate corrective actions?
- Did the Registered Entity arrange for individuals with full knowledge of the matter to meet with MRO if/when asked to do so?

- Did the Registered Entity volunteer its relevant findings and provide all relevant evidence regarding the possible violation?
- Did the Registered Entity’s disclosure include the full scope of the possible violation?
- Did the Registered Entity’s disclosure include the identification of all steps taken upon learning of the possible violation, and the related corrective actions?
- Did the Registered Entity’s disclosure include all communications among involved employees and/or third parties?
- Did the Registered Entity’s disclosure include the identity of employees involved, including senior management?
- Did the Registered Entity’s disclosure include all documents evidencing the possible violation?
- Did the Registered Entity uncover the possible violation itself through its own self-evaluation, internal audit, or internal compliance program?
- Does the Registered Entity clearly understand and acknowledge that any unjust profits it may have realized as a result of the violation must be quantified and disgorged?

At the December 2010 MRO Compliance Enforcement Workshop, it was suggested that MRO consider developing or sharing Models of Excellence identified in the Compliance and Enforcement processes. Toward that end, MRO is providing a “scrubbed” version of an actual Self Report received in 2010. This Self Report emulates excellence in reporting to MRO staff and warrants significant consideration in the penalty determination as it evidences a strong internal compliance program.

The following Self Report clearly identifies the Entity, the Reliability Standard(s) in question, what the possible violation is, what caused it, the immediate and long-term corrective actions [mitigation], and the potential impact this possible violation has on the BPS [severity level]. All important pieces of a good Self Report.

If you have any questions regarding a Self Report, please contact [Sara Patrick](#) or [Wayne VanOsdol](#).

(Continued on page 4)

Sample Self Report – 2010

Entity Name: Unnamed Registered Entity (URE)

Standard Requirement: CIP-006-1 R1.8

Physical Security Plan—The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at the minimum, the following:

R1.8. Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009.

Description and Cause:

URE is reporting a violation of CIP-006-1 R1.8. Under this requirement, the access control system must be treated as a Critical Cyber Asset. In violation of this requirement, individuals that have not received CIP training and a Personnel Risk Assessment (PRA) as required by CIP-004-1, R3, were allowed cyber access to the Access Control system database, ProWatch.

The ProWatch application is the system which is used for physical access control. ProWatch consists of control boards, keycards, card readers, alarms and is configured via two servers, ProWatchA and ProWatchB. The system operates with one primary active server and one backup server in the standby mode. At the time of the discovery, ProWatchA was the active server.

The event was discovered on December 8, 2009, while preparing to make the six month password change on the ProWatch access control system server, as required by CIP-006-1, R1.8. The ProWatch Administrator, while performing the password change, identified that a group called "Domain Admins" was part of the local administrator group the ProWatchA server. Based on his knowledge of the system, the ProWatch Administrator investigated further to ensure that all members of this group were authorized users. His investigation determined that some members of the Domain Admins group were unauthorized users; i.e. did not have the required training or PRA. His investigation also determined that the Domain Admins did not have access to the ProWatchB server, which at the time was in standby mode.

Further investigation revealed the unauthorized group, Domain Admins, had been automatically added to the ProWatchA server when the server was rejoined to the network sometime after April 27, 2009, but prior to July 1, 2009.

Immediate Corrective Actions:

Immediately upon discovery, the group in question, Domain Admins, was removed from the ProWatchA server administrator group. A security check was performed and it was discovered that one Domain Admin user had accessed the server on one occasion when the server was in standby mode. At the time the ProWatchB server was the active server and the Domain Admin group was not present on it.

The Domain Admin who had accessed the server was verifying the patch status of the server, which is a routine task. The individual should not have been able to log on to the ProWatchA server. The individual involved recalls finding a discrepancy while checking the patch status on the server, so she logged on to the server to verify the status. Interviews with the individual determined she had no malicious intent when she logged onto the server.

Weekly reviews of the database auditing reports verified that no unauthorized manipulations to the access control database occurred.

Cause of the Event:

Background: Currently the Corporate access control system, ProWatch, includes all NERC access points. Because the access control system is used corporate wide, the ProWatch servers are located on the corporate domain and are supported by Corp IT. The energy management system is located on a separate secure domain maintained by the Energy Management IT group.

Prior to mandatory compliance for R1.8 of CIP-006, access to ProWatchA and ProWatchB was removed for all users who had not been given CIP training and successfully completed a PRA, as required by CIP-004. Although unauthorized users were removed from the server in preparation for the July 1, 2009 compliance date; the procedures and processes used to assure software control of the servers had not been implemented. Prior to July 1, 2009 and prior to implementing the software procedural and process controls, problems were identified with the ProWatchA server. To remedy these problems, the server was rejoined to the corporate network domain. When the server was rejoined to the domain, the Domain Admins group was automatically added to the local administrator group. The function of automatically adding the Domain Admins group to the local administrators group when joining a Windows server to a domain is programmed into the operating system by Microsoft.

Corrective Actions:

1. Obtain training and PRA for Server & Storage team as well as the Domain Admins group.
 - Each person on the Server & Storage team as well as those in the Domain Admins group will be trained and have a PRA completed. If the server has to be rejoined to the domain, those people in the Domain Admins group will meet CIP-006 R1.8 standards.
2. Maintain list of Server & Storage team as well as the Domain Admins group which will be reviewed on a quarterly basis.
 - A list of people on the Server & Storage team as well as the Domain Admins group will be kept by Corporate Security and reviewed on a quarterly basis to meet CIP-004 R4.1 standard.
3. Configure new ProWatch servers dedicated to controlling access to NERC areas. This will result in the Energy Management IT group becoming responsible for the servers and eliminate Corp IT support. The individuals on the Server & Storage team and in the Corp IT Domain Admins group will no longer have access to ProWatch servers.

Potential Impact to the Bulk Power System:

The potential impact on the Bulk Electric System was negligible. Although a window of vulnerability existed; the complexity of the system, its inherent security, and the ability to detect changes assured the reliability and safety of the BES.

To access the ProWatch application, a user ID must be defined in the application and the workstation used to access ProWatch must also be tied to that particular user. The Domain Admins did not have a ProWatch ID nor a workstation associated with their ID, and therefore did not have access to the ProWatch application.

Individuals with Domain Admins rights did have access to the ProWatch database. A highly skilled individual with Domain Admin access rights could have used database tools; e.g., SQL Server Administrator, to manipulate the database to allow unauthorized access. This scenario is highly unlikely because of the complexity of the ProWatch database schema. An improperly implemented update to the database would have resulted in the failure of the database management system to properly mount the ProWatch database and automatic notification of the ProWatch administrator would have occurred. In the unlikely event that the database was successfully changed, it would have been detected during weekly reviews of database changes performed every Monday.

Given the complexity of modifying the database to obtain unauthorized and undetected access; the potential but unrealized threat to the safety and reliability of the BES was negligible. The initial assessment of this event determined that the event was not reportable since the Domain Admins could not have accessed the access control system, ProWatch. However upon further review by the Internal Compliance Oversight Committee, it was determined that improbable scenarios existed that could have allowed manipulation of the database, and allowed unauthorized physical access to Critical Areas.

Demonstrating Compliance with Certain CIP Standards

(Continued from page 4)

CIP-003

Responsible Entities should be prepared to demonstrate that they are making their cyber security policy available to contractors and service vendors, as well as employees. CIP-003 (versions 1 through 3) R1.2 requires a Responsible Entity to ensure that “[t]he cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.” While CIP-004 (versions 1 through 3) R2.1 requires the Responsible Entity to establish, maintain, and document an annual cyber security training program that “will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.” Although CIP-003 R1.2 does not expressly reference contractors and service vendors, it is contradictory to the shared goal of improving reliability and protecting Critical Cyber Assets to limit the application of CIP-003 R1.2 to employees only. Consistent with the requirement in CIP-004-1, R2.1 to provide cyber security training to contractors and service vendors, in addition to employees, Responsible Entities should ensure that contractors and service vendors, in addition to employees, have access to the cyber security policy which typically spells out their respon-

sibility for proper use and protection of Critical Cyber Assets.

CIP-009:

Some Reliability Standards, such as CIP-009, require that Responsible Entities exercise a plan/conduct drill “at least annually.” Some Entities are requiring in their plans that a drill be conducted “once per calendar year.” Depending on the date of mandatory compliance with the Standard, the Entity may inadvertently become noncompliant. For instance, an Entity required to comply with CIP-009-1, Requirement 2 as of July 1, 2008, that conducts a drill on June 1, 2009 would satisfy the annual drill requirement in the Standard. However, if the Entity has stated in its Recovery Plan that a drill will be conducted “once per calendar year,” it must complete a drill by December 31, 2008 to avoid a finding of noncompliance.

There are numerous other places where ‘annual’ shows up in the CIP standards. An ‘unofficial’ count has found the word annual showing up in no less than 23 different places within the CIP standards. Having a defined use of the word annual in a documented compliance program is a good measure to demonstrate that a Registered Entity understands how the term is being applied within its organization.

Enforcement “Case Notes” Available to Stakeholders

Concurrent with the release of this Newsletter, MRO Enforcement staff posted a document entitled “Case Notes” to the MRO [website](#). This document provides a brief description of violations processed by MRO, describes the risk each violation posed, and describes what action was taken to mitigate the concern. The document includes examples for each of the Top 10 Most Frequently Violated Standards in the MRO Region.

The MRO Compliance Committee assisted in the development of this document and provided valuable feedback. MRO staff will be updating the document on a quarterly basis, so please check back regularly. For questions regarding this document, please contact [Sara Patrick](#), Director of Regulatory Affairs and Enforcement.



NERC posts lessons learned and webinars on their newly created Resource Center

NERC recently created a [Resource Center](#) that makes educational products available to Regional Entities, industry participants, and regulators. These products 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.

Currently, you will find information on upcoming Webinars, past Webinars, Lessons Learned, and past NERC presentations.

NERC Compliance Application Notices

Also on NERC’s website, you will find [Compliance Application Notices](#) or CANs. The NERC Compliance Operations Program and the Regional Entities are working together toward a common goal to improve consistency, transparency, and efficiency of compliance processes. One way that NERC is working to achieve this goal is by providing different types of notices that provide compliance information about queries and items that arise from the field and industry, and Compliance Application Notices (NERC CANs) are one type of notice.

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. NERC Compliance Operations will use CANs to help:

- Provide transparency
- Identify trends
- Educate and engender a culture of compliance
- Improve consistency
- Encourage effective self-policing and correction

OPERATIONS UPDATE

Dan Schoenecker, VP Operations

A Year in Review

2010 was another busy year in the MRO region. A new Operating Committee (OC) was formed to provide greater focus on issues related to operations and that are being addressed by the NERC Operating Committee. The OC is responsible for review of disturbance reports and event analysis efforts, seasonal assessments and post seasonal assessments from an operational perspective, as well as providing a forum for discussion of bulk power system issues and best practices.

Also in 2010, the Protective Relay Subcommittee (PRS) was asked to review the procedures and categorization of protection system mis-operations. Mis-operations have been identified as one of the causal factors in most system events across North America. As a result, NERC and the Regions are developing metrics to help identify specific cause categories in an attempt to reduce the number of mis-operations by addressing the most common causes.

MRO's Board of Directors have considered and support an accelerated asset replacement program for the MRO Region related to protection systems. The program is intended to educate and share best practices amongst Registered Entities and to assist in planning and budgeting for replacement of aged or outdated protection facilities and equipment. In 2010, MRO performed a more extensive analysis of mis-operations according to three relay types: Electro-mechanical, Solid State and Microprocessor-based. The initial results of this analysis were reported to the board and can be found in the December 2nd board meeting [agenda packet](#), Item 15a.

We hope to continue this work and develop ideas on how to best address protection system replacement (e.g. priority, avoiding types of failures, best practices for settings of micro-processor based relays) to finalize the program document. We want to thank the stakeholders who participated on the analysis team—it cannot be done without you! Hopefully the work can be expanded in 2011 as a way to help Registered Entities improve system reliability and address potential risks.



Event Analysis

NERC, through the Event Analysis Working Group (EAWG), developed new processes, procedures and templates for Regional and Registered Entities to use in the review of disturbances and events impacting the

Bulk Electric System. A field trial began on October 25, 2010, and will continue into early 2011. Lessons learned from the field trial will be incorporated into the processes, reporting categories and templates, and eventually updates to the NERC Rules of Procedure will be drafted to reflect the new Event Analysis processes. Public reports of events that

occur in the MRO Region are posted on the MRO website at www.midwestreliability.org.

Assessments

MRO worked with NERC and the other Regions to re-align the footprints of periodic assessments from the Regional Entity boundaries to planning authorities. MRO staff believes that aligning assessments with the entities responsible for planning is more meaningful to the reader of reports.

The 2010-2011 Winter Assessment has been completed and is now posted on the NERC [website](#).

Additionally, the 2009-2010 Post-Winter Assessment has been posted on the [NERC website](#). The 2009-2010 Post-Winter Assessment is the first of its kind and is reported on a Reliability Coordinator basis. The goal of this report is to provide a look-back to see how the system performed, compare actual demand to forecast demand, etc. Although weather was quite typical in the MRO region, the TX and FL regions experienced unusually cold winters. For example, the ERCOT region experienced an actual peak demand that was 28% higher than the seasonal forecasted demand. The next post-seasonal assessment will be starting soon and will provide a look-back at Summer 2010.

In the first few weeks of January 2010, MRO will be sending out requests to Planning Authorities registered within the MRO Region to collect data for the 2011 Long Term Reliability Assessment and the 2011 Summer Assessment. Note that for 2011, these assessments will be organized on a ISO/RTO/Planning Authority basis. Load and Generation data will no longer be collected from individual companies/utilities as in past years, but instead it will be collected through the Planning Authorities. In this manner, planning reserves and other reliability metrics will be captured more accurately since they will be on a Planning Authority basis instead of a Regional Entity basis.

NERC also recently completed a scenario assessment called [Resource Adequacy Impacts of Potential U.S. Environmental Regulations](#). The consultant group Energy Ventures Analysis Inc., was hired by NERC to perform this study. The impacts of four potential EPA regulations are considered in this scenario report:

- 1) Clean Water Act – Section 316(b), Cooling Water Intake Structures
- 2) Title I of the Clean Air Act – National Emission Standards for Hazardous Air Pollutants (NESHAP), or Maximum Achievable Control Technology (MACT) Standards;
- 3) Clean Air Transport Rule
- 4) Coal Combustion Residuals

The report indicates that the MRO region could be significantly impacted by these potential regulations, due to the predominance of coal units within the region.

Lessons Learned

At the last board meeting, Mark Davis, Director of Asset Management for American Transmission Company, presented best practices related to vegetation management. His presentation can be found in Item 9 of the December 2nd annual MRO Board and Member meeting [agenda](#)

(Continued from page 6)

[packet](#). Staff would like to thank Mark for sharing his very informative presentation! The MRO Board plans to include a “Reliability Excellence” segment at future board meetings as well.

Looking Forward to 2011

Many of the projects started in 2010 will continue into 2011. Additionally, MRO has a major undertaking planned to review transmission clearances as required by the recent NERC alert titled “[Consideration of Actual Field Conditions in Determination of Facility Ratings](#).”

STANDARDS UPDATE

Carol Gerou, Standards Manager

Taking The Lead

In 2007, FERC Order 693 directed Registered Entities to meet fill-in-the-blank standards as a matter of good utility practice. In paragraph 297, FERC stated:

“The Commission requires supplemental information for any Reliability Standard that currently requires a regional reliability organization to fill in missing criteria or procedures. Where important information has not yet been provided to us to enable us to complete our review, we are not in a position to approve or remand those Reliability Standards. Accordingly, we will not approve or remand such Reliability Standards until the ERO submits further information. Until such information is provided, compliance with fill-in-the-blank standards should continue on a voluntary basis, and the Commission considers compliance with such Reliability Standards to be a matter of good utility practice.”

To encourage the development of enforceable NERC Reliability

The newly approved Underfrequency Load Shed (UFLS) standard will result in a shift in responsibility for UFLS program analysis and implementation. MRO staff held a conference call on the matter and the newly approved standard can be viewed on NERC’s [website](#). Staff expects regulatory approval shortly.

In closing, MRO staff needs your help and asks for your engagement. Please consider volunteering for a committee, working group, or standards SME team—just ask us if you want to volunteer. We can match your interest with a need within MRO or NERC.

Standards that address fill-in-the-blank standards, MRO is taking the lead to develop and submit Standard Authorization Requests (SARs) and associated draft standards for two topics: 1) special protection systems (merging the NERC Reliability Standards: PRC-012, PRC-013, PRC-014, & PRC-015) and 2) misoperations of protection systems (merging the NERC Reliability Standards: PRC-003, PRC-004, & PRC-016). The SARs and proposed standards were initially developed by NERC’s Regional Reliability Standards Working Group (now called “NERC’s Regional Standards Group” or “RSG”) but work on these SARs and associated draft standards has slowed.

To expedite these SARs and their associated draft standards, MRO staff will review and revise these drafts and submit them to the RSG and ask the RSG to endorse them.

Vacancies exist on the MRO Standards Committee

If you are interested in serving on the MRO Standards Committee or as a Standards Committee Subject Matter expert (SME), please contact [Jennifer Matz](#) for a nomination form and instructions on how to submit. Open positions can be viewed on the Standards page of MRO’s [website](#).

FINANCE UPDATE

Sue Clarke,
VP of Administration and Finance



2010 Recap

In our 2010 end-of-year projections, staff anticipates actual and budget will be in line or slightly over budgeted costs.

While the budget included costs for additional work related to CIP and TFE management, these costs were budgeted as consulting costs. Staff re-evaluated the workload and determined that staff would be used for the majority of CIP work with external consultants used only to manage workload peaks. Overall, CIP efforts were greater than budgeted, but staff was able to find savings in other areas to offset the overage. CIP related matters accounted for approximately 30% of the budget in 2010.

2011 Outlook

At this point, MRO staff believes that the 2011 budget will be “tight” as a result of several factors. These factors include

added follow-up work on CIP spot checks conducted in 2010, additional training and education materials (result of feedback from the 2010 regional survey of Registered Entities), staff follow-up on the NERC FAC alert, and enhancements to the 2011 CMEP implementation plan. At this time, staff believes that the budget can be managed to the approved levels with certain savings which have already been identified; but, staff sees more risk for a budget overage in 2011 than in previous years.

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.

COMPLIANCE UPDATE

Wayne VanOsdol, VP Compliance

MRO 2010 Winter Reliability Workshop

Staff would like to thank the 145 attendees that participated in the MRO Reliability Workshop on December 1, 2010, in Bloomington, MN. All workshop materials and presentations can be found on MRO's [website](#).

Below are questions received from workshop attendees and MRO staff's related responses. If you have any follow-up questions or comments, please contact the [MRO Compliance Department](#).

Q: *Regarding the Administrative Citation Process – Why is this process not included as part of the NERC/MRO 2011 Implementation Plan?*

A: The Administrative Citation Process was formally presented to the NERC Board of Trustees Compliance Committee on November 3, 2010, and subsequently shared with FERC staff for consideration and review. MRO supports NERC's plan to submit the first Administrative Citation filing in January, 2011. The 2011 Implementation Plan is an annual plan, submitted by November 1 of each year to NERC for approval in accordance with NERC Rules of Procedure Section 401.6. Page 30 of the MRO 2011 Implementation Plan references the Administrative Citation Process and states:

"Throughout 2011, MRO will take steps to streamline the process and provide more certainty sooner. MRO supports the development of alternative processes, including an administrative citation approach to resolve minor violations."

Q: *Are we to understand that there will continue to be two self-certifications each year? If so, is there a timeframe other than Spring and Fall? (Looking for specific month due to MRO).*

A: The actual annual self-certification dates and procedures (spring and fall) will be posted on the MRO compliance web site in early 2011. Typically, the spring self-certification will be conducted in May and the fall in October.

Q: *Why are there two self-certifications, when the requirement is for an "annual" self-certification?*

A: NERC requires all Registered Entities to participate in the annual self-certification. MRO does not require two self-certifications, but rather there are two separate time periods to provide the annual self-certification. The reason for conducting two periods is to ensure we are not requesting Registered Entities to participate in the annual self-certification during the same time in which they are receiving a compliance audit. The fall annual self-certification is the default in which all Registered Entities participate. However, if a Registered Entity is scheduled to receive a compliance audit during the period of time in which the fall annual self-certification is being conducted, then that entity will be scheduled to participate in the spring annual self-certification. This ensures that multiple compliance monitoring methods (self-certification and audit) are not initiated or conducted for the same Registered Entity at the same time.

Q: *Regarding performance observations in the 2011 Implementation Plan. If a Registered Entity is not on the 2011 schedule for an audit, is it correct to assume that the Registered Entity could still be subject to a performance observation? If yes, what is the difference, if any, between a performance observation and a spot check?*

A: At this time, MRO plans to initiate the performance observations by collecting various work plans and schedules from Entities scheduled to receive a compliance audit in 2011. However, if there is some type of scheduled event (such as a restoration training drill) planned for Entities that are not scheduled to receive an audit in 2011, we could certainly consider attending the performance observation which would potentially reduce the audit scope for the associated Entities in 2012.

Q: *Does MRO believe that even though the defined term "protection system" is NOT in standard PRC-008, all elements of the protection system are included in PRC-008, or does PRC-008 only apply to the underfrequency relays themselves in MRO's perspective? Keeping in mind, PRC-005-2 treats UFLS differently than a typical BES protection system.*

A: NERC Standard PRC-008-0 requires the Registered Entity to identify UFLS "equipment". There are a number of components which are common to Protection Systems and UFLS equipment; however, these are typically at a lower voltage. MRO has identified 4 pieces of equipment essential for the UFLS program: the relay, the PT (source of frequency), the DC circuitry, and the battery. Similarly, in reference to NERC Standard PRC-005-2, the new standard recognizes: relays, communication systems, voltage transformers, station DC supply and control circuitry. PRC-005-2 does identify the maximum intervals for these components, which in the case of batteries, are different than the batteries associated with the other Protection Systems.

Q: *Why does NERC and MRO use BPS and BES interchangeably when they are two different definitions? This occurs throughout all documents, even in the mitigation plan document and is extremely confusing, as well as annoying.*

A: MRO staff has used these terms interchangeably in the past, and we will attempt to be more careful in the use of this terminology. NERC and MRO use the NERC statement of Compliance Registration Criteria for identifying owners, operators, and users of the interconnected bulk power system. The NERC Statement of Criteria document includes the NERC definition of the [bulk electric system](#). MRO has adopted the NERC BES definition, however, there may be other Regional Entities that have developed their own definition of BES.

As a reference point, Commission (U.S.) [Order 693 A](#), Section II.A.1, describes the difference between the BES and BPS. On November 18, 2010, FERC directed NERC to revise its definition of the Bulk Electric System to ensure that the

(Continued from page 8)

definition encompasses all facilities necessary for operating an interconnected electric transmission network. That order can be found on FERC's [website](#).

Q: For reliability standards such as PRC-007 that require data submittal to MRO within a specified time frame (30 calendar days) but MRO allows for additional time, such as an extra week, would an Entity be found in violation if they submitted the required data in the MRO time frame but beyond the 30 calendar days specified in the requirement?

A: While late or incomplete data submission for certain standards (not regulatory approved) may not be subject to enforcement action, MRO expects all data to be submitted on time and tracks submittals that are late or incomplete. MRO's time frame is the time frame identified in the Standard. Late submittals cause delays in summarizing data or completing work that the data is used for and creates extra work for staff and Entities. MRO staff has tried to be accommodating in the past whenever possible. Going forward, however, MRO will implement a process similar to what is used in the CMEP for data submittals that are not received on time. More information will be available as this process is developed.

Q: In regards to Susan Court—does FERC plan on shortening up their time frame when it comes to taking action on a standard once it has been approved by the NERC Board of Trustees (BOT)?

A: MRO and Ms. Court do not speak for the Commission (FERC). However, FERC has placed an emphasis on the need for change to the NERC Standards Development Process. Based on the increased level of interest in the NERC Reliability Standards process, it is likely that FERC will reduce the time it takes to approve a proposed or revised Standard. However, current efforts underway with the NERC Standards Committee and Drafting Teams should result in more Standards being proposed or revised. An increased number of Standards for consideration may result in delays in approval.

Q: MRO should consider, and then propose to NERC if they agree, the following suggestion to modify the audit time frames in 2 ways:

1) Self-certification should be for a calendar year, rather than September to September. The self-certification would occur in February for the previous calendar year.

A: MRO will consider this suggestion, thank you. Please refer to [MRO's report](#) to NERC on the implementation of the 2009 Compliance Monitoring and Enforcement Program, which details MRO's self-evaluation of the CMEP implementation and includes suggestions for improvements.

2) On-site compliance audits that would occur every three years. These audits would cover the previous three calendar years. If a potential violation were discovered, then the Registered Entity could look at the current year as well, else they would not. Whether an audit occurs in March or October, only the previous three complete calendar years would be reviewed. This approach would accomplish two things: a) allow the audit time frame to be more understandable rather than May 2008 (the last

on site audit) to November 2011. b) Allow the audited entities to better pull together the requested information to send to the Regional Entity with a more clear understanding of what the Regional Entity wants to look at. Registered Entities could better prepare and make the audits smoother for everyone. For example: the Registered Entity self-certified for September 2009–September 2010, an on-site audit then occurs in June 2011. In order to do this, I believe that MRO requests the entity to perform another self-certification from September 2010–May 2011. By modifying the audit time frames (as discussed above), no second self-cert would occur.

A: MRO will consider the suggestion. The monitoring period for the annual self-certification is not the same as the monitoring period of the audit. In the example above, MRO would have requested the entity to participate in the fall annual self-certification (September 2009 to September 2010). Also, the example indicates that this Entity is scheduled to receive a compliance audit in June 2011. The monitoring period for this audit ends on the date in which the exit briefing (close date of audit) is presented, and goes back to June 18, 2007 if needed or back to the registration date.

That said, going forward MRO auditors plan to review the internal controls, procedures, and processes in place at the time the audit is being conducted, and go back in time only as deemed necessary. For example, if the related evidence of controls, procedures, processes presented to the auditors were newly created documents, it would be logical for the auditors to request copies of the previous versioned documents. This is to obtain reasonable assurance that controls were in place prior to the audit being conducted. Evidence of compliance is typically not collected for the annual self-certification, therefore, there is no duplication of data collection. Also, the monitoring periods (period of time) for any one compliance audit and annual self-certification do not align. The self-certification pertains to a defined twelve-month period and the audit can have a more extended period depending upon the situation.

Additionally, MRO does not believe an entity that is scheduled to receive a compliance audit during the calendar year should also participate in the annual self-certification. Ideally, that Entity would receive a waiver on self-certification since they're scheduled to receive an audit. MRO attempted to implement this process and was directed by NERC to require all Registered Entities to participate in the self-certification regardless of whether they are scheduled to receive an audit.

Summary

MRO staff appreciates all of the comments, questions and suggestions received as a result of the workshop. The more we (Regional and Registered Entities) work together, the better and more transparent our processes will become.

The Mid-Continent Compliance Forum (MCCF) held a meeting concurrent with the MRO Reliability Workshop. The MCCF provides a forum for Registered Entities to share compliance materials as well as compliance audit experiences. MRO staff sincerely appreciated the opportunity to present information at the MCCF December meeting. MRO staff recommends that Registered Entities attend workshops, seminars, and other related meetings where power system reliability and associated compliance matters are discussed.

Please continue to watch for additional workshops and seminars to be held by MRO Reliability Assessment and Standards departments in 2011.

CMEP Report

Compliance Monitoring and Enforcement Program

MRO CMEP Program Update
4th Quarter, 2010

Wayne VanOsdol, Vice President Compliance

Compliance Statistics

- 102 Total violations discovered through implementation of the CMEP and reported to NERC in 2010
- 20 Compliance audits scheduled and conducted in 2010; all compliance audits completed on-time as planned
- 17 CIP spot checks scheduled and conducted in 2010; all CIP spot checks completed on-time as planned

The 2011 audit and CIP spot-check schedule is posted on the MRO web site at: http://www.midwestreliability.org/02_compliance/audit_information/MRO_Compliance_Audit_Schedule.pdf

Annual Implementation Plan Update

The 2011 annual implementation plan and associated compliance audit schedules (and other monitoring methods) can be found on the MRO website ([MRO 2011 Implementation Plan.pdf](#)). A key item to note in 2011 includes program improvements which begin using a risk and performance based compliance audit approach. The approach is used to determine the scope of Reliability Standards to be reviewed during the audit. The 2011 plan and associated changes are the first step for moving to the risk/performance approach.

In the past, the majority of the audit included a review of documents, procedures, and plans (a paper audit). The review of this documentation is important and will continue for certain Reliability Standards having a high risk / high impact to system operation. The performance approach improves the compliance program by allowing auditors to observe the implementation of internal controls. Performance or field observations can occur in a number of ways, such as observing various work being performed in the field, or training being conducted. These program changes benefit all involved. The overall ERO model and compliance program is improved through the actual observation of internal control implementation, and through the observation of training sessions (such as a restoration drill), which may potentially include a number of Reliability Standards through the observation of one training session. This could mean fewer standards reviewed during the audit since the associated evidence was reviewed during the field observation. The next step for program advancement is to quantify or measure the effectiveness of a Registered Entity compliance program. This outcome would result with an audit scope determination that is specific to each Registered Entity. In 2011, MRO (with the assistance of Registered Entities) will be developing a methodology and assessment process that will be used for determining the effectiveness of a Registered Entity compliance program; it is MRO's hope that these efforts will be combined with those of NERC and other regions.

Annual Self-Certification Update

As required by the NERC Annual Plan, all Registered Entities must participate in the annual self-certification being conducted by MRO in the Fall of 2011. In addition, MRO will conduct an annual self-certification in the spring for those Registered Entities that are scheduled to receive a compliance audit during the same timeframe in which the Fall self-certification is scheduled. Procedures for the annual self-certification (spring and fall) are currently under development. MRO staff will notify all Registered Entities once procedures are posted on the MRO web site (also referenced on page 8-Workshop Questions and Answers).

CIP- Technical Feasibility Exception (TFE – Part B Update)

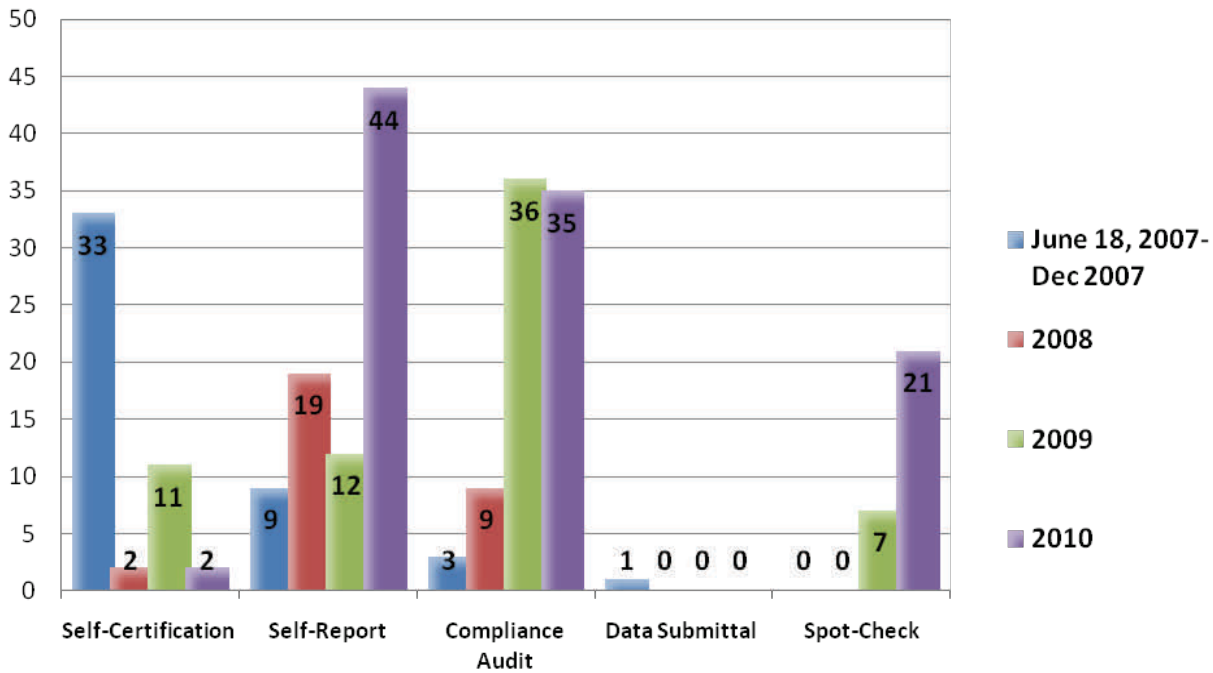
The TFE Part B assessment work continues. MRO is processing TFE's from 20 Registered Entities totaling 302 TFE's that cover 7,288 assets. MRO expects to complete the Part B assessment within the 365 day review period (within the first quarter 2011).

webCDMS Update

MRO has developed criteria for user names in webCDMS. This helps determine and track the user associated with the Registered Entity. The criterion MRO defined is: Entity Acronym_LastName. For example: MRO (entity acronym)_McNabb (last name of user). If you do not know your company acronym, please contact Jo Anne McNabb (651-855-1730). We ask that you continue to use this naming convention when creating users in the webCDMS compliance and enforcement tool. 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.

(Continued from page 10)

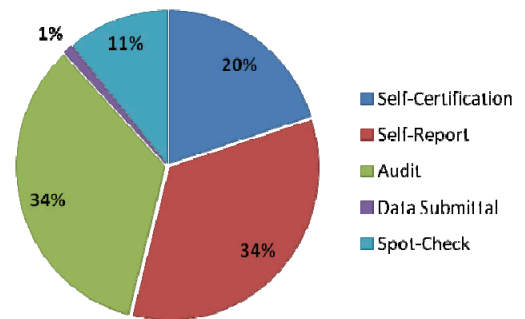
Discovery Methods Yearly Comparison (numbers below include dismissals)



Discovery Methods

Discovery Method Detail	June 18 - Dec 2007	2008	2009	2010	Sub Total	(less) Dismissed	Total
Self-Certification	33	2	11	2	48	14	34
Self-Report	9	19	12	44	84	15	69
Compliance Audit	3	9	36	35	83	18	65
Data Submittal	1	0	0	0	1	0	1
Spot-Check	0	0	7	21	28	11	17
Totals	46	30	66	102	244	58	186

Percentage Comparison (inception-to-date)



Standards Most Frequently Violated

Standards Most Frequently Violated	Frequency	% to Total
PRC-005-1 Trans. and Gen. System Maint. and Testing	54	29%
PRC-008-0 Implementation and Documentation of UFLS Equip. Maintenance Program.	23	12%
CIP-004-1 Cyber Security-Personnel and Training	19	10%
FAC-003-1 Vegetation	13	7%
CIP-001-1 Sabotage Reporting	11	6%

*Dismissals not included

Alleged and Confirmed Violations

MRO staff continues its validation of alleged violations that are identified through the eight discovery methods (compliance audit, self-certification, random spot-check, compliance violation 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 Alleged and Confirmed Violation Process

	Total ⁽¹⁾	%
Total Number of Alleged Violations	244	100%
Less: Number of Dismissals	58	24%
Less: Number of Violations Processed ⁽²⁾	84	34%
Less: Number of Violations Awaiting NOP	31	13%
Number of Violations Outstanding ⁽³⁾	71	29%

1) Numbers are a cumulative total at the end of current quarter

2) Accepted or approved by applicable regulator, includes settlements

3) Includes both alleged and confirmed violations yet to be processed and approved by applicable regulator (244 less 58 (Dismissed) less 84 (accepted and/or approved by regulator) less 31 (viols awaiting NOP) = 71)

Status of Mitigation Plans

Mitigation Plans	
Number of Violations with Mitigation Plans	139
Number of Violations with Completed Mitigation Plans (validated by MRO staff)	119
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	47

The following is a brief overview of the MRO Compliance and Enforcement staff activities during the 4th Quarter 2010:

- **31** new alleged violations were submitted to NERC
- **15** alleged violations were dismissed
- **16** PNAVs for 38 alleged violations were issued
- **3** NAVAPS for 3 alleged violations were issued
- **2** NOCV's for 2 confirmed violations were issued
- **1** Deficiency Notice for 1 confirmed violation was issued
- **6** Administrative Citations for 16 confirmed violations were issued
- **8** NOPs were filed for 17 violations
- **2** Settlement Agreements for 6 violations were submitted for BOTCC consideration

For past quarterly reports on MRO Compliance and Enforcement, please refer to the [CMEP Updates](#) on MRO's Compliance Monitoring & Enforcement website page.

(Continued from page 2, From the President)

violations outside the existing Compliance Monitoring and Enforcement Program (CMEP) to properly categorize minor matters and align risk and materiality with efforts.

- 2) Distinguish between self reports resulting from an effective compliance program, even repeat violations, and self reports resulting from a happenstance discovery or in preparation for an audit. This distinction is important because, all other things equal, a Registered Entity with a strong compliance program poses less risk than an entity with a weak program.

Overall, we can do more by providing education and insights on reliability matters and share key learnings from system events, enforcement actions, and studies/assessments sooner. A survey of Registered Entities conducted by MRO in November highlighted the need for more education and training. In 2010, we started to do more of this through newsletters, workshops and one-on-one dialogues with Registered Entities, and this remains a key initiative for 2011.

The Future

We must continue to challenge ourselves to improve the current process of discussing, negotiating and creating new reliability standards. We need the process of adopting new reliability standards to be faster, more effective and have assurance that the standards are technically sound. Additionally, the reliability standards themselves must focus on meaningful improvements and “gaps” to the reliable operation of the bulk power system. MRO supports NERC’s current efforts to create processes that are responsive to regulatory directives,⁹ as well creating more streamlining of these processes. However, we cannot allow discussion about the process for adopting new reliability standards, or the current process itself (the administrative), impede the improvement of reliability and mitigation of risks. In this regard, we believe that a Registered Entity must focus on reliability as the goal or “doing the right thing.” The imprecision of an existing reliability standard or the lack of a reliability standard should not get in the way of the Registered Entity addressing legitimate risks to the bulk power system.

MRO staff also believes that improving reliability and proactively addressing risks depends, in part, upon NERC and MRO’s ability to quickly disseminate information such as lessons learned and recommendations from event analyses. This key initiative remains for MRO in 2011 and is an integral part of our education efforts for stakeholders in the region. MRO will also continue to emphasize mitigation through its compliance and enforcement processes as an effective means of improving reliability. When violations of reliability standards occur, our staff will focus on how to best address the matter through corrective actions to improve reliability and ensure future compliance, all the time, in a collaborative manner with the Registered Entity.

Additionally, MRO’s evaluation of compliance must evolve

beyond paper audit and reliance on interviews of subject matter experts. Field observation and more testing will be required to really increase the level of rigor and due diligence across the ERO model, raising the bar of performance. MRO is taking some initial steps in this direction in 2011.

Finally, compliance must be an instrument of reliability, not the opposite. Or, as a FERC Commissioner recently put it “reliability is the master of compliance, not the reverse.” To this end, Registered Entities must develop cultures that value reliability, not unlike INPO’s inculcation of the value of safety in the nuclear industry.¹⁰ For example, a formalized ability, or core competency, to quickly evaluate a “blip in the night” in a transparent fashion may prevent the “bump in the night” we all want to avoid. This is an inherent part of a culture of reliability. We need to define and recognize strong compliance programs and let the strength of the compliance program influence the scope of our work (i.e., an important consideration of risk). As I testified before FERC:

“...compliance must be an instrument of reliability, not the opposite”

[W]e should recognize those Registered Entities with strong compliance programs in the scope of [MRO’s] work and scale the work accordingly. This isn’t about trust, it’s about risk. Strong compliance programs, less risk. Weak compliance programs, more risk.”¹¹

We welcome your thoughts on indices of a strong compliance program as an element of a good culture of reliability. We think it begins with tone at *and from* the top which can be defined as “a visible willingness by senior management to let values drive decisions, to prioritize those values above other factors (including financial results), and to expect all others in the organization to do the same.”¹² Embracing reliability to the full extent will mean that senior management is developing and monitoring reliability-compliance with reliability standards is just one of the measurements. Some of the program elements MRO staff considers in its evaluation are:

- Does senior management regularly evaluate reliability?
 - Are there established metrics?
 - Is it considered as part of the organization’s enterprise risk management program?
 - Is the organization proactively addressing aging workforce issues, particularly as the issues relate to the organization’s technical workforce?
 - Are management’s financial incentives properly aligned around compliance?
- Does the entity have well understood written procedures to analyze system events, including EMS outages?
- What are the policies and procedures on self reporting a potential violation?
 - Does it consider the risk of “being caught” in deciding whether to self report?
 - Are there ways in which self-reporting is encouraged?

⁹ See for example, http://www.nerc.com/fileUploads/File/PressReleases/PR_procedure_16_Dec_10.pdf

¹⁰ See footnote 6, supra.

¹¹ Reliability Monitoring, Enforcement and Compliance Issues Remarks of Daniel P. Skaar, President, Midwest Reliability Organization on November 18, 2010, AD11-1-000. Technical conference testimonies can be viewed on FERC’s [website](http://www.ferc.gov).

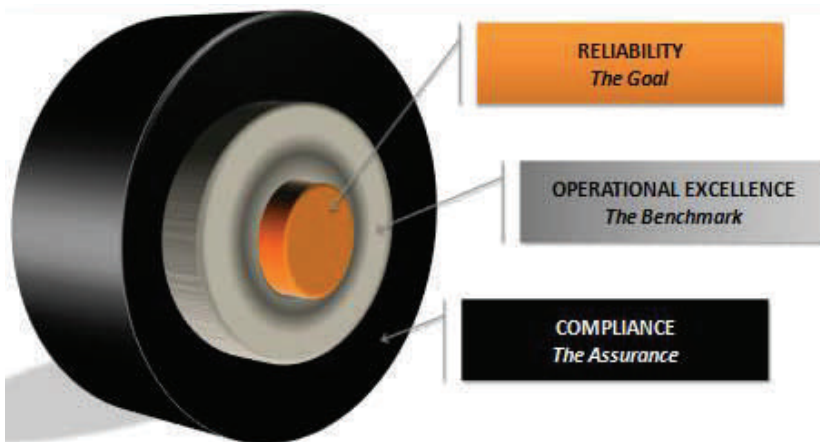
¹² Howard Sklar, then Vice President of Compliance & Ethics at American Express, see <http://www.compliancebuilding.com/2009/03/27/ethical-integrity-leadership-setting-the-tone-from-the-top>

(Continued from page 13, From the President)

- Are there ways in which self-reporting is discouraged?
- Is the organization reporting and analyzing mis-operations in a timely manner? Are there sufficient resources devoted to finding out the root cause of the mis-operations? Are corrective actions taken in a timely manner with documentation?
- Is there an effective training program for grid operators?
 - Do grid operators train on simulators?
 - Are there tests?
 - Is there communication training?
 - Are communications monitored and periodically evaluated?
- Is the vegetation management program effective? Has the program been measured or evaluated in its effectiveness through peer reviews or through an independent party?
- Is your personnel “cyber security savvy?”¹³ (A culture of security will a topic in the next newsletter.)
- Have you clearly defined the roles of vendors and contractors related to standards to assure responsibilities with compliance?

Figure 1 below further demonstrates the relationship between reliability and compliance. Reliability should be the center of a good compliance program.

Figure 1



Conclusion

MRO staff is committed to helping the industry improve reliability and address risks. Compliance is an instrument of reliability – and we recognize it as part of the answer. MRO would like to see compliance so deeply embedded into an entity’s operations that compliance is a minimum measure of reliability.

A commitment to strong self assessments and addressing risks proactively can naturally foster a culture of strong reliability. MRO staff believes that an entity that embraces reliability as a value embedded in their culture and has invested in a strong compliance program poses less risk—and that in the future this should be taken into consideration in the scope of all of our work as a reward for “getting it right.”

In conclusion, MRO staff believes the regulatory model passed by Congress and accepted by Canadian jurisdictions is a strong foundation that leverages industry expertise and can assure reliability matters are prioritized correctly and addressed appropriately—so that there are no “bumps in the night” like the cascading outages of 2003.

¹³ Cyber security is considered a public safety issue and is being addressed by a number of agencies including the Department of Defense, Homeland Security, Department of Energy as well as FERC. We believe it will require significant commitment of time and resources in the future.

Quote of the Month

“No government at any level and for any price can afford the police necessary to assure our safety and our freedom unless the overwhelming majority of us are guided by an inner personal code of morality.”

- Ronald Wilson Reagan

IMPORTANT INDUSTRY UPDATES AND EVENTS

NIAC publishes final report on Critical Infrastructure Resiliency

The Department of Homeland Security's [National Infrastructure Advisement Council](#) (NIAC) submitted its final report titled "A Framework for Establishing Critical Infrastructure Goals" to President Barak Obama on October 19. The final report can be found on the [NIAC](#) website.

MRO President comments on the FERC November 18 Technical Conference

MRO President, Daniel P. Skaar, submitted his [remarks](#) to FERC in December regarding the November 18 FERC technical conference on Reliability Monitoring, Compliance and Enforcement Issues.

FERC announces Technical Conference on Smart Grid Interoperability Standards

Washington, D.C., December 20, 2010

FERC announced that it will host a Technical Conference on Monday, January 31, 2011 on Smart Grid Interoperability Standards (RM11-2-000) at its corporate headquarters in Washington DC. A free webcast will be available via FERC's [website](#).

FERC announces Technical Conference on Priorities for Addressing Risks to Reliability of the Bulk-Power System

Washington, D.C., December 20, 2010

FERC announced that it will host a Technical Conference on Tuesday, February 8, 2011 on Priorities for Addressing Risks to the Reliability of the Bulk-Power System (AD11-6-000) (Washington, DC) (Free webcast available). A free webcast will be available via FERC's [website](#). To read Commissioner Norris' statement regarding this Technical Conference, please visit: <http://www.ferc.gov/media/statements-speeches/norris/2010/12-16-10-norris.asp>

FERC removes barriers to development of needed transmission in Midwest Region

Washington, D.C., December 16, 2010

The Federal Energy Regulatory Commission (FERC) today approved a proposal that removes barriers to the development of much-needed transmission that will help maintain the reliability of the transmission grid and deliver cleaner and cheaper energy to consumers across the Midwest.

The proposal, offered by the Midwest Independent Transmission System Operator Inc. (Midwest ISO) and its stakeholders, is intended to enable the region to comply with energy policy mandates and to address reliability and economic issues affecting multiple transmission zones within the region. This proposal improves Midwest ISO's ability to ensure that the costs of transmission projects with regional benefits are properly assigned to those who benefit. The full press release can be found on FERC's [website](#).

NERC Board passes Rules of Procedure modifications

WASHINGTON, DC - The Board of Trustees for the North American Electric Reliability Corporation (NERC) passed a modification to the Rules of Procedure that will give the board the ability to address regulatory directives from the Federal Energy Regulatory Commission (FERC) should the need arise, while maximizing the opportunities for stakeholder participation in the standard development process. Read the full [press release](#).

The Rules of Procedure can be found at <http://www.nerc.com/page.php?cid=1|8|169>

NERC releases "Reliability Considerations from the Integration of the Smart Grid" report

WASHINGTON, DC - To reach the potential of the smart grid while maintaining continued power system reliability, industry will need new tools and models to support planning and operations of the bulk power system. Further, bulk power system operators will need increased visibility and dispatchability as smart grid innovations change the character of distribution systems, says a North American Reliability Corporation (NERC) report released on December 2nd, 2010.

The report - [Reliability Considerations from the Integration of Smart Grid](#) - is a high-level, preliminary assessment of potential reliability considerations. In addition, it outlines a work plan for coordinated actions from the electric industry to enable integration of smart grid devices and systems resulting in a secure and reliable bulk power system.

FERC Approves the NERC/MRO Delegation Agreement and Revised Bylaws

On October 21, 2010, in Docket Number RR10-11-000, the Federal Energy Regulatory Commission (FERC) accepted the revised delegation agreements between the North American Electric Reliability Corporation (NERC) and the eight Regional Entities, including Midwest Reliability Organization (MRO), pending minor revisions. Included in the docket were MRO's amended and restated bylaws that were previously approved by the MRO Board, the MRO Members and NERC. The amended and restated bylaws were approved by FERC with one minor revision, which was subsequently approved by the MRO Board at the annual meeting on December 2nd, 2010.

The revised bylaws can be found at MRO's website at: http://www.midwestreliability.org/01_about_mro/overview/by_laws/MRO_Bylaws.pdf. MRO's Policies and Procedures were also revised to reflect the bylaws and can be found on MRO's website at: http://www.midwestreliability.org/ABO_policies_procedures.html

MRO Comments on ReliabilityFirst's Proposed Planning Resource Adequacy Standard

On December 29th, MRO provided comments to FERC on docket RM10-10-000, regarding RFC's Planning Resource Adequacy Standard. The docket can be found on FERC's [website](#). MRO's comments can be found on MRO's [website](#).

Innovative Smart Grid Technologies Conference

The second Conference on Innovative Smart Grid Technologies (ISGT 2011), sponsored by the IEEE Power & Energy Society (PES), will be held January 17-19, 2011 at the Anaheim Hilton in Anaheim, California. For more information, visit <http://www.isgt2011.com/site/>

Related Links:

[Department of Energy](#)

[Federal Energy Regulatory Commission](#)

[North American Electric Reliability Corporation](#)



MRO Employee 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)

External Affairs & Public Relations

[Miggie Cramblit, Director of EA and PR](#) (1721)

Finance

[Sue Clarke, VP of Finance & Accounting](#) (1707)
[Regina Davis, A/P & A/R](#) (1706)

Enforcement

[Sara Patrick, Regulatory Affairs, Counsel and Enforcement Director](#) (1708)
[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

[Clark Liu, IT Manager](#) (and CIP Program Manager) (1744)

After Hours Emergency Line
651-734-8355

EMPLOYEE NEWS

Jennifer Matz and husband Nick welcomed a health baby boy into the world on November 23. **Christian Nicholas Matz** weighed in at 6 lbs, 11 oz and 19 inches long.

Congratulations Jennifer and Nick!

Riaz Islam, MRO Engineer, married Yen Doan Thai on January 1st, 2011 in Saint Paul, Minnesota.

Congratulations Riaz and Yen!

Also, please welcome the following new employees to MRO:

Kristine Hutchens joined MRO in December as the **Operations Administrator**. Kristine fills the position previously held by Jennifer Matz, who accepted an opening as the Standards and Mitigation Administrator.

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

ABOUT MRO

MRO is a non-profit organization dedicated to ensuring the reliability and security of the bulk power system and operates under delegated authority from regulators in both the U.S. and Canada. MRO works to develop and ensure compliance with regional and international standards and also performs assessments of the grid's ability to meet the demands for electricity. Additional information can be found on our website at www.midwestreliability.org

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 Inter-connection-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
Feb 8	TBD	Compliance Committee Meeting	Holiday Inn Select Bloomington, MN
Feb 16	TBD	MRO Planning Committee Meeting	TBD
Feb 17	TBD	MRO Standards Committee Meeting	MRO Offices Roseville, MN
Feb 21 Feb 22	12:00 - 5:00 8:00 - 12:00	Protective Relay Subcommittee Meeting	Holiday Inn Select Bloomington, MN
Feb 22	TBD	MRO Operating Committee Meeting	TBD
March 15	8:00 - 4:00	Model Building Subcommittee Meeting	Holiday Inn Select Bloomington, MN
March 24	TBD	Board of Directors	TBD

MRO Mission

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

MIDWEST RELIABILITY ORGANIZATION
2774 Cleveland Ave N.
Roseville, MN 55113

Ph: 651-855-1760
Fx: 651-855-1712
www.midwestreliability.org