Issue 3
2018 May/June

RELIABILITY FIRST

INSIDE THIS ISSUE

ReliabilityFirst Corporation
3 Summit Park Drive
Suite 600
Cleveland, OH 44131
Main Phone: (216) 503-0600

Web: www.rfirst.org
Follow us on

A Note from the President

Tim Gallagher, President and CEO

Dear Stakeholders:

Happy Summer!

I would like to draw your attention to the recap of a panel discussion from the CIP portion of our Spring Workshop. Based on one of our identified CIP Themes, we facilitated an engaging panel with a few entities to discuss breaking down organizational silos. They provided some great insight in addition to practical strategies that they have implemented. Another approach to improving your organizations security posture by breaking down silos, is keeping those at top engaged and aware.

Relatedly, in our last newsletter, I mentioned I would be starting a new initiative to reach out to the CEOs in our footprint, and I've since issued the first Leadership Letter. My hope is that this proactive initiative to share critical information I encounter helps ensure all of our CEOs stay engaged. Below are the questions I posed last month to your CEOs in response to seeing insufficient ownership, awareness, and preparedness as primary contributing causes to deficient security postures.

1. Do you personally know who is assigned the ultimate responsibility for Operational Technology and Information Technology security in your organization? Do they know it, too?
2. How comfortable are you that you understand the strengths, weaknesses, and threats associated with your Operational Technology and Information Technology security postures?
3. Operational Technology security should be staffed, trained, and equipped to fight the next battle, not just the previous one. Does your security staff drill their responses frequently to ensure they are ready to deal with any threat? Have you seen the results of any of these drills?

I did not ask for responses to these questions, but intended them to facilitate internal dialogue on this topic I find particularly important. I will continue to share these succinct, high-level letters with your CEOs when I see matters that I feel are truly important. I also reminded all of your leaders that the RF Team is available to your organization and can assist with evaluations and custom training on reliability, security, or compliance topics. This issue also includes updates to the CIP Standard on Cyber Security Management Controls (CIP-003-7) and resources, including a Lighthouse article, that thoughtfully explores these revisions and their implications. I hope these, and all of our communications, help break down silos and spur dialogue throughout your organizations and across our Region and the ERO as we all continue collaborating to keep the lights on.

Forward Together,

Tim

From the Board

RF Holds Second Quarter Board of Directors Meetings in Cleveland, OH

From left to right, Steve McElwee and Bryon Koskela


From left to right, Sue Ivey and Tim Gallagher


Mike Bryson

RF held its Second Quarter Board of Directors meetings at its offices in Cleveland, OH from May 23-24, 2018. RF staff and special guests provided presentations on various topics. Highlights included the following:

- During the Compliance Committee meeting, Bryon Koskela and Steve McElwee from PJM Interconnection, LLC (PJM) provided an overview of PJM's recent CIP security network segmentation project to continuously improve the security of PJM's operations. They described the drivers for network segmentation and the high-level process for achieving this segmentation.
- During the Board of Directors meeting, the Board adopted a resolution in recognition of Sue Ivey's service on the Board from 2005-2018. Sue Ivey served as an RF Board member since the corporation's inception in 2005, and she recently retired from the Board. Ms. Ivey was in attendance at the meeting, and the Board thanked her for her commitment, dedication, and contributions to RF and its mission.
- Jason Blake provided an update regarding the pending Rule 1208 request filed by Wisconsin Public Service Corporation and Upper Michigan Energy Resources Corporation to transfer from MRO to RF. He led a discussion on the activity to date related to this Rule 1208 request, and on the next steps in the process.
- Michael Bryson, Board member and Vice President of Operations at PJM, presented and led a discussion on PJM's analysis of the reliability implications of FirstEnergy's recent generation retirements.

RF Board of Directors

and

Committee Meetings

will be held

at the RF offices in

Cleveland, OH

August 29-20, 2018.

2018 Spring Workshop

A very special thank-you to all who attended and participated in RF's Spring 2018 Workshop, April 24-26 at the Nationwide Hotel & Conference Center in Columbus, OH. We had 228 attendees join us in person and via WebEx.

The first day was primarily dedicated to situational awareness, specifically the loss of EMS tools and applications. RF was pleased to introduce guest speakers from industry (Sam Chanoski from E-ISAC, Jule Tate and Dr. Wei Qiu from NERC) along with our own subject matter experts to explain the impact of these EMS outages in the RF footprint. We hope that you had the following take-aways from the EMS portion:

1. If you have had EMS fall-downs in the past, you are not alone. This is the most common reportable event in the RF footprint with approximately 25-30 new category 1h events each year. When these happen, the RF Events Analysis and Situational Awareness Department is more than happy to help you analyze the circumstances of the event to reduce occurrences and durations.

From Left to right, Jule Tate and Dr. Wei Qiu

If additional help is needed, consider talking to RF's Entity Development group about a targeted appraisal. Information about EMS outages is located on our new EMS Knowledge Center located on our public website, including the NERC reference document Risks and Mitigations for Losing EMS Functions.

2. A common theme across the RF footprint is the loss of EMS tools and applications other than SCADA (control and indication). We are seeing more and more State Estimator outages, which impacts the ability to run Real-Time Contingency Analysis.

   When these happen, do not forget to inform your Reliability Coordinator so that they can help you monitor your system while you recover from the outage. Modeling external data has been a key theme to these outages so RF is working with NERC to publish new Lessons Learned documents (stay tuned!)

3. Denise Hunter provided a presentation on Internal Controls. While she used an EMS-related example to illustrate her point, internal controls are critical to all of the reliability work performed every day. Simply, how do we ensure what we want to happen – happens, and what we don't want to happen – doesn't happen.

   Please see the article on page six for more details regarding implementing an internal controls program.

Denise Hunter

Continued on page 4

2018 Spring Workshop

Continued from page 3

4. When making a significant change to your EMS, don't forget to contact Entity Development. A recertification may be needed.

5. For more information on all-things EMS-related, consider attending NERC's Sixth Annual Monitoring and Situational Awareness Conference, October 2-3, hosted this year by MISO. NERC will send out the details regarding registration in June.

   This conference provides a more detailed look at EMS innovations and emerging technologies, Lessons Learned from past events, plus a vendor panel consisting of ABB, GE, OSI, and Siemens to answer any and all EMS questions you may have!

   If you have interest in helping plan this event, or want to assist industry in studying the causes and impacts of EMS outages, consider joining or participating on the NERC Operating Committee's EMS Working Group.

For more information on EMS outages or the Event Analysis Process in general, see our website.

The second day of the Spring Workshop was devoted to private meetings for RF's Compliance User Group (CUG) and Critical Infrastructure Protection Committee (CIPC).

Our CIP Workshop was held on the last day and included CIP Themes, Patch Management, GridEx IV, Modifying CIP Standards, and Threat Intelligence. See Breaking down Silos on the next page for a full recap of our panel.

The last day also included a presentation on Industrial Control Threat Intelligence from Sergio Caltagirone of Dragos, Inc.

Sergio provided an overview of the threat environment in which adversaries are outpacing defenders, as well as a detailed explanation of Threat Intelligence and its benefits.

Attendees learned how to use Threat Intelligence to reduce harm by improving decision making before, during, and after cybersecurity incidents, and why Threat Intelligence should be an integral part of any modern cybersecurity program to significantly improve the efficacy of all existing elements.

2018 Spring Workshop

Breaking Down Silos

At our recent Spring Workshop, RF was fortunate to host a panel of experts from three Registered Entities who discussed strategies to address potential organizational silos.

Organizational silos was one of four themes identified in a joint report recently published by RF, SERC Reliability Corporation, and Western Electricity Coordination Counsel (the "Regions"), available here. The purpose of the report was to identify themes in terms of program deficiencies that have made it difficult for some entities to maintain a successful CIP compliance program.

The panelists shared their experiences and why they found it necessary to actively address silos. They discussed the benefits of operating without silos, including improved security as well as efficiency gains as a result of operating under a single program and using the same tools across an organization.

Each panelist also offered many practical resolutions to prevent and address organizational silos.

- For example, Exelon holds an annual CIP week where personnel from across the organization come to one location for a week to review and update all of the entity's CIP program documents.
- WEC Energy Group discussed its use of a single compliance database to track all control activities, including CIP and non-CIP activities across the organization.
- Additionally, MISO explained how it leverages its Requirement Owners by embedding them throughout the organization to ensure consistency and increase communication between groups.

Thank you to our panelists for sharing their time and valuable insight.

"You can't eliminate all of the silos. The key is making the silos communicate and making them as small as possible."

Tom Breene - Manager Federal Regulatory & Policy
WEC Energy Group

"CIP Week reduces the risk of organizational silos by concurrently engaging line performers and key managers across Exelon business units in the review of proposed changes to the Exelon CIP program."

Bill Edwards – Assistant General Counsel
Exelon

"Best practices are more likely to emerge when you can get organizational silos communicating with each other."

Kristina Pacovsky - Managing Sr. Corporate Counsel
MISO

Internal Controls Paradigm Shift

By: Denise Hunter, Senior Technical Auditor

Introduction

The ERO Compliance Monitoring program is an integral process to ensure the reliability and resiliency of the Bulk Electric System. Over the course of time, the monitoring program has matured and shifted from being a compliance based plan to a process that is risk based and incorporates internal controls. Through the use and review of internal controls, an organization can protect its assets, ensure accurate reporting of data and compliance with the policies of the ERO, Region and the entity, and evaluate its performance. The following is part one of a two part series on internal controls.

Elements of Internal Controls

Effective internal controls provide reasonable assurance regarding the accomplishment of the established objective. Internal control programs are generally comprised of the five components detailed below. Each component is important in its own right, and all components should be constantly evolving.

1. Control Environment

The control environment is the foundation of the internal control program. The control environment is how the organization addresses various aspects of company activities that include, but are not limited to, leadership philosophy, ethical values, policies, procedures and how management empowers their employees. The control environment embodies how the organization as a whole, from the CEO to the new employee, perceives, approaches and embraces the internal control program. Examples of the control environment include: company policies and procedures, anonymous hot lines, and vertical communication practices.

2. Risk Assessment

Assessing risk is a critical component of an internal control program. An organization must first establish their company objectives in order to determine the risks that would preclude the organization from achieving those objectives. Then the organization can move towards identifying the risks that could cause harm to the organization. This is not always an easy process. The organization must ensure it performs a risk analysis for both internal and external sources. The groundwork for an entity's risk assessment should include the risks associated with its registered function and the risk the entity poses to the BES. Because change is inevitable due to economics, regulatory and operating conditions, the organization must ensure it has implemented mechanisms capable of dealing with the risks associated with change.

The process of identifying and analyzing risk is an ongoing process. A constant assessment of an organization's risks should be performed in order to identify the impact the changing risk has on established internal controls. By consistently reviewing external and internal risks, an organization positions itself with the appropriate mechanisms needed to react timely to changing conditions.

3. Control Activities

Control activities, or internal controls, are the activities an organization performs to ensure its established objectives are achieved. They are the mitigating actions an organization takes to address identified risks.

There are two types of control activities, key and non-key. Key control activities are those activities that if they are not performed, or performed incorrectly, will result in a process failing or providing inaccurate data. Non-key controls are secondary activities that, should they fail, will not affect the process. Examples of internal controls include activities as diverse as reviews, change management, incident documentation, authorizations, verifications, security of assets and segregation of duties, to name a few.

4. Information and Communication

Organizations require accurate, timely, pertinent information in a form and time frame that enables people to carry out their responsibilities. Effective communication flows down, across and up an organization. In order for internal controls to be embraced and taken seriously, the message must be provided in a clear, consistent manner from all levels of management. All employees must understand their role in the internal control program, as well as the importance their individual activities play as they relate to the work of others. Finally, it is imperative that employees are provided a means of communicating significant information upstream.

5. Monitoring

Internal control programs can only be effective if they are monitored. The breadth of the risk that the control is designed to mitigate will determine the scope and frequency of evaluation. Monitoring must be appropriately performed in order to ensure that the control continues to be effective and produce expected results. The assessment of all key controls performance over time, either in a formal or informal manner, must be performed in order to ensure that the control is performing as designed and producing expected results. Monitoring can occur in a variety of ways, either during the ordinary course of operations, it can be an established, defined process that includes management and supervisory activities. The monitoring process should start with establishing a baseline to determine normal performance, identifying the appropriate data to be collected, determining thresholds that initiate an alert, analyzing data to provide actionable insight and finally accurately reporting to all appropriate stakeholders.

Organizational risk changes over time, therefore so must internal control programs. The introduction of new technology, personnel, and regulatory demands can dilute once effective controls. Monitoring internal control programs aid in identifying those issues.

Data Visualization

By: Kellie Anton, Senior Analyst-Data Analytics

Treemaps, What They Are and How to Use Them

In this installment of the series on data visualization, we will present a newer type of visualization, the treemap.

Treemaps are an effective means of displaying hierarchical data, data with groups, and subgroups. The treemap does this by creating a ranked set of nested rectangles. Recall from the first installment on pie charts that humans can assess rectangles for the relative area rather quickly; the treemap capitalizes on this cognitive strength. The treemap does this in a ranked order with the most significant contributors to the top left and the smallest to the bottom left.

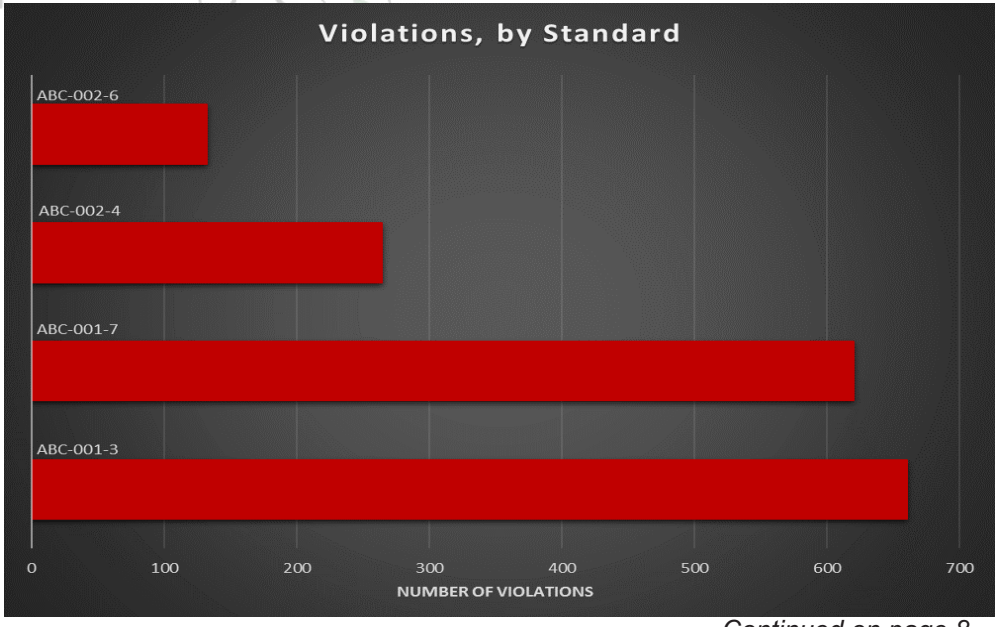
When might one use the treemap? Tree maps work great:

- To display large amounts of hierarchical data.
- When a bar chart cannot adequately handle a large number of values.
- To show proportions between each part and the whole.
- To show the pattern of the distribution of the measure across each level of categories in the hierarchy.
- To show attributes using size and color coding.
- To spot patterns, outliers, most-important contributors, and exceptions.

We will start off with the horizontal bar chart from the last article, Violations by Company.

This graph gives a nice view of the violations by company. Now perhaps we also have the number of violations by standard. We could show that similarly.

We now have some new insight, Violations by Standards. Standard ABC-001-3 is the most violated standard, and the Umbrella Corporation has the most violations. What if we wish to know who violates what standards the most? This is where we can use the hierarchical prowess of the treemap.



Continued on page 8

Data Visualization

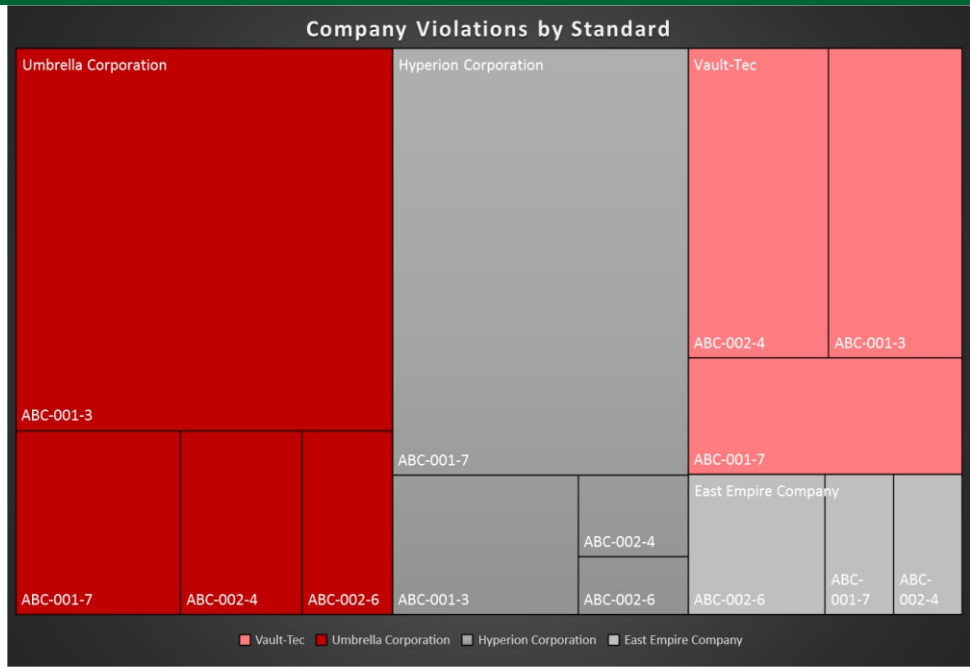
Continued from page 7

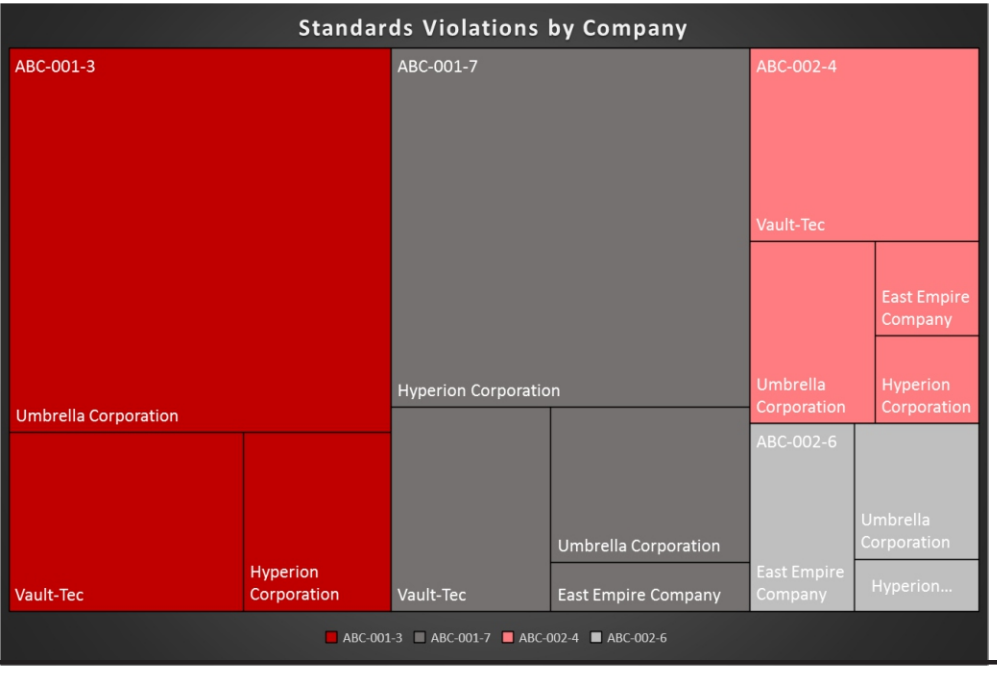
We will examine which standards are most violated and which companies violate those standards.

We can quickly see the structure of the treemap. ABC-001-3 is to the left as the most violated standard, and we can quickly see Umbrella Corporation violated this standard more frequently. Similarly, we also can see that the East Empire Company did not violate this standard. We can also see that ABC-002-6 is violated the least by its size and position. Here we see that East Empire Company violated the standard the most and that Vault-Tec has not violated this standard.

We could rearrange the hierarchy to look at this a different way. To the right is the same data presented differently to tell a different story. We can still see the same principles in use and the top-left to bottom-right ordering of the categories and sub-categories.

Treemaps are a powerful tool for visualizing data and telling some quick data stories. They also work exceptionally well as part of a dashboard where they can tell a bigger story alongside other visualizations. As of Office 2016, Excel can handle this job; there is no longer a need for a business intelligence (BI) tool or a program such as R or Python to make Treemaps. You will find the treemap under the Insert tab. Go to Charts and find Insert Hierarchy Chart and have fun looking at your data in a new way.





"How to Make a Treemap in Excel," Laptop, https://www.laptopmag.com/articles/make-treemap-excel
"Treemaps in Power BI," Microsoft, https://docs.microsoft.com/en-us/power-bi/power-bi-visualization-treemaps

Summer 2018

By: Tim Fryfogle, Senior Engineer- Reliability

Reliability Resource Risk Assessment

RF performs a seasonal summer resource adequacy assessment based on the results PJM and MISO provide. This article shares some highlights from MISO, PJM, and RF assessments. For the upcoming summer of 2018, both MISO and PJM are expected to have an adequate amount of resources to satisfy their respective planning reserve requirements. Below are the statistics that supports our analysis on outage risk, which concludes that there should not be an issue supplying demand within the RF Region this summer.

PJM Capacity and Reserves

- PJM net capacity resources that include existing certain generation and net scheduled interchange for the 2018 planning year are projected to be 189,859 MW. The projected reserves for the PJM RTO during the 2018 summer peak are 46,846 MW, which equates to a 32.8 percent planning reserve margin for the net internal demand (NID) of 143,013 MW. This is greater than the PJM planning reserve margin requirement for the 2018 planning year of 16.1 percent. The planning reserve margin for this summer is higher than the 2017 forecast level of 27.9 percent. This is due to increased capacity in PJM's market and a slightly negative percent load growth compared to last year.

MISO Capacity and Reserves

- MISO net capacity resources for the 2018 planning year are 141,417 MW. The current projected reserves for MISO for the 2018 summer peak are 22,703 MW, which equates to a 19.1 percent planning reserve margin for the NID of 118,714 MW. This is greater than the MISO planning reserve margin requirement of 17.1 percent for the 2018 planning year. An increase in the amount of generator forced outages is responsible for the change in the planning reserve margin requirement. The planning reserve margin for this summer is slightly higher than the 2017 forecast level of 18.8 percent. This is mostly due to decreased demand in MISO's market that have taken place since last summer.

RF Footprint Resources

- The net capacity resources in the RF footprint for the 2018 planning year are projected to be 204,012 MW. The projected reserves for the RF footprint during the 2018 summer peak is 41,035 MW. The Total Internal Demand (TID) of 173,407 MW with demand side management of 10,430 MW equates to a NID of 162,977 MW. Since PJM and MISO are projected to have adequate resources to satisfy their respective reserve margin requirements, the RF region is projected to have sufficient resources for the 2018 summer period.

Random Generator Outage Risk Analysis

The following analysis evaluates the risk associated with random outages that may reduce the available capacity resources below the load obligations of PJM or MISO.

The stacked bar charts in Exhibits 1 and 2 are based on forecasted Summer 2018 demand and capacity resource data for the PJM and MISO RTOs. The daily operating reserve requirement for PJM and MISO at the time of the peak demand is also included as a load obligation. The range of expected generator outages is included for scheduled and random outages. The random outages are based on actual NERC Generator Availability Data System (GADS) outage data from June, July, and August of 2013 through 2017.

The committed resources in PJM and MISO are represented by the Resources bar in shades of blue and only include the net interchange that is a capacity commitment to each market. Additional interchange transactions that may be available at the time of the peak are not included as they are not firm commitments to satisfying each RTO's reserve margin requirement.

The firm demand and the demand that can be contractually reduced as a Demand Response are shown in shades of green. The firm demand constitutes the Net Internal Demand, with Total Internal Demand including the Demand Response. The daily Operating Reserve requirement (shown in yellow) is between the NID and DR bars. There are two sets of stacked Demand bars on the chart, one each representing the 50/50 demand forecast and the 90/10 demand forecast. For instance, the 50/50 demand forecast projects a 50 percent likelihood that demand exceeds 143,013 MW. The 90/10 demand forecast is a more conservative model, projecting a 10 percent chance that demand exceeds 154,501 MW. Since DR is utilized first to reduce the load obligation when there is insufficient capacity, this part is at the top of the Demand bar. In the event that utilization of all DR is not sufficient to balance capacity with load obligations, system operators may first reduce operating reserves prior to interrupting firm load customers.

Between the Resources bar and the Demand bars is the Outage bar. While scheduled outages during the summer season are generally minimal, there are scheduled outages planned during the summer that are reflected in the amount of Scheduled

Continued on page 10

Summer 2018

Continued from page 9

Maintenance (colored gray) in the Outage bar. The remainder of the Outage bar represents the entire range of random outages (pink shows 100 percent of the random outages; rose shows less than 100 percent down to 10 percent of the random outages; and red shows less than 10 percent down to 0.2 percent of the random outages on the chart) which occurred during the five-year reference period.

In the following discussion of the random outages, the analysis of random outages exceeding certain reserve margin targets is presented as a probability. These probabilities are not based on a true statistical analysis of the available daily random outage data. Rather than statistical probabilities, these numbers represent the percentage of the daily outages during the five prior summer periods that would have exceeded the reserve margin that is listed. They are discussed as probabilities as a matter of convenience in describing the analysis results.

To the left side of the range of random outages are probability percentages related to the amount of random outages that equal or exceed the amount of outages shown above that line on the Outage bar. Moving from top to bottom of the Outage bar represents an increasing amount of random outages, with a decreasing probability for the amount of random outages. In the PJM chart, the random outages represented by the bar above the 100% point is 6,310 MW. This means that the probability of there being at least 6,310 MW of random generation outages is 100 percent.

Similarly, at the 10 percent point, the outages represented by the bar above the 10 percent point is 19,746 MW (6,310 MW + 13,436 MW). There is a 10 percent probability that there will be at least 19,746 MW of outages. As shown by the probabilities and corresponding amounts of random outages, the distribution of random outages is not linear throughout the range of outages observed.

To the right of the Outage bar are the probabilities of the random generation outages that correspond to different levels of demand obligation.

Exhibit 2 contains the information to perform the same analysis for MISO. The top of the 50/50 demand obligation bar for MISO represents TID with operating reserves. The line between the Outage bar and the 50/50 Demand bar represents a 3 percent probability that there will be an amount of outages that will require Demand Response resources to be utilized.

The top of the 90/10 demand obligation with the operating reserves has a 41 percent probability that Demand Response will be required. With the listed Demand Response fully utilized, there is a 2 percent probability that the random outages will reduce available resources below the firm demand and operating reserve obligations.

Exhibit 1 - 2018 Summer PJM Outage Risk Chart

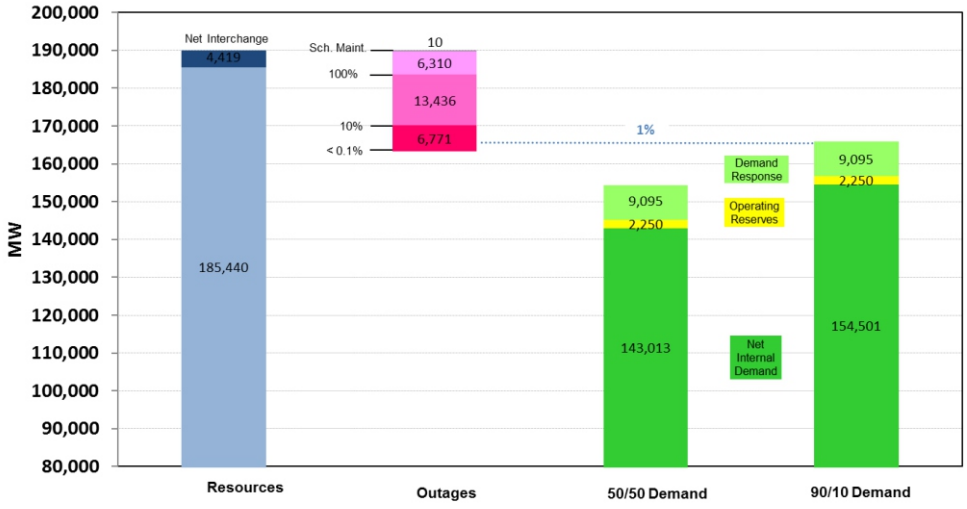
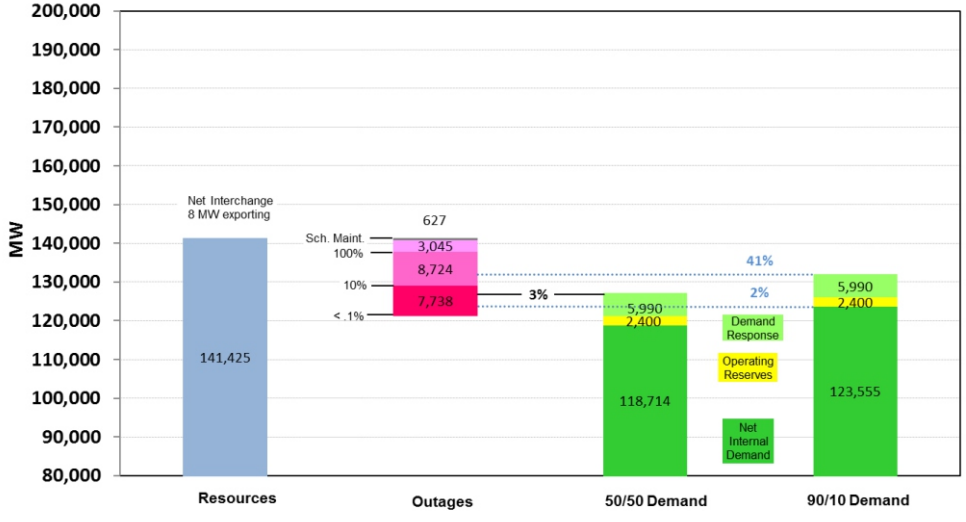


Exhibit 2 - 2018 Summer MISO Outage Risk Chart



CIP Low Impact Update

FERC Order 843 Approves CIP-003-7

On April 19, 2018, the Federal Energy Regulatory Commission (FERC) issued Order 843 (available here) which, in addition to other actions, approved CIP-003-7 (available here.)

This article will discuss the provisions of Order 843 and will also summarize the changes between CIP-003-6 and CIP-003-7.

Order 843 took these actions:

1) FERC approved Reliability Standard CIP-003-7, Cyber Security – Security Management Controls.

2) FERC approved the associated implementation plan, violation risk factors, and violation severity levels.

3) FERC directed NERC to conduct a study to assess the adequacy of the implementation of electronic access controls for low impact BES Cyber Systems. This study is to be completed by June 30, 2021.

4) FERC directed NERC to modify CIP-003-7 to include a clear requirement to mitigate the risk of malicious code from third-party Transient Cyber Assets.

Summary of Changes between CIP-003-6 and CIP-003-7

Changes in Terminology

Two terms were removed from "Glossary of Terms Used in NERC Reliability Standards" (NERC Glossary, available here):

- Low Impact BES Cyber System Electronic Access Point (LEAP)
- Low Impact External Routable Connectivity (LERC)

Two existing NERC Glossary terms were modified to accommodate their use for low impact BES Cyber Systems:

- Transient Cyber Asset (TCA)
- Removable Media

Requirement R1 Part 1.2, Cyber Security Policy for Assets Containing Low Impact BES Cyber Systems

The required topics for the cyber security policy for assets containing low impact BES Cyber Systems have changed. The Version 6 policy topic "Electronic access controls for Low Impact External Routable Connectivity (LERC) and Dial-up Connectivity" has been simplified to "Electronic access controls." Two policy topics, "Transient Cyber Assets and Removable Media malicious code risk mitigation" and "Declaring and responding to CIP Exceptional Circumstances" have been added. Each of which is further discussed below.

Attachment 1 Section 2, Physical Security Controls

The section covering physical security controls was modified to remove the reference to LEAP and substitute equivalent language that does not refer to LEAP.

Attachment 1 Section 3, Electronic Access Controls

Section 3 was re-written to remove the terms LERC and LEAP, and to clarify the electronic access control requirements. Some sections of Order 843 provide insight into FERC's expectations. Order 843 P 28 states, in part, "We [FERC] expect responsible entities to be able to provide a technically sound explanation as to how their electronic access controls meet the security objective."

Also, Order 843 P 29 includes the statement, "[W]e believe that NERC and the Regional Entities will have the ability to assess the effectiveness of a responsible entity's electronic access control plan as well as a responsible entity's adherence to its electronic access control plan." Responsible entities should be cognizant of these statements when developing and implementing electronic access controls for low impact BES Cyber Systems.

Attachment 1 Section 4, Cyber Security Incident Response

The only change in Section 4 is the accommodation of the name change of the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) to the Electricity Information Sharing and Analysis Center (E-ISAC).

Attachment 1 Section 5, Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation

CIP-003-7 Attachment 1 Section 5 is a new provision that requires responsible entities to "achieve the objective" of mitigating the risk of malicious code from Transient Cyber Assets and Removable Media for its low impact BES Cyber Systems.

Continued on page 12

CIP Low Impact Update

Continued from page 11

Violation Severity Levels

The Violation Severity Levels were modified to reflect the new language in Requirement R1 and Attachment 1.

Attachment 2

Attachment 2 was modified to reflect the changes in Attachment 1

Guidelines and Technical Basis

In the Guidelines and Technical Basis (G&TB), text was added to discuss the cyber security policy requirements for low impact BES Cyber Systems. The G&TB was also modified to reflect the changes to Attachment 1. Discussion of electronic access controls was greatly expanded, and the associated Reference Models were re-written and expanded to correspond with the new language of Section 3.

Implementation Plan

Order 843 also approved the CIP-003-07 Implementation Plan. In accordance with the Implementation Plan, CIP-003-6 Requirement R2 Attachment 1 Sections 2 and 3 (physical security controls and electronic access controls) will not become effective on September 1, 2018. Instead, CIP-003-7 Requirement R2 Attachment 1 Sections 2 and 3 will become effective along with the rest of CIP-003-7 on January 1, 2020.

The Implementation Plan also incorporates by reference the sections of the CIP-003-5 and CIP-003-6 Implementation Plans that deal with planned and unplanned changes, carrying forward these provisions into CIP-003-7.

As the CIP-003-7 Implementation Plan is silent on initial performance of periodic requirements, the initial performance date for CIP-003-6 Attachment 1 Section 4.5's Cyber Security Incident response plan testing remains April 1, 2017.

Electronic Access Control Adequacy

Order 843 P 30 requires NERC to perform a study to assess the adequacy of the implementation of electronic access controls for low impact BES Cyber Systems. The results of this study are to be submitted to FERC no later than June 30, 2021. When audits of CIP-003-7 begin in 2020, audit teams will begin gathering data for this study to be submitted to NERC.

Mitigation of Malicious Code

Order 843, P 39 directs NERC to modify CIP-003-7 to include an explicit requirement that responsible entities implement controls to mitigate the risk of malicious code that could result from third-party transient electronic devices.

Summary

The table below summarizes the CIP requirements that are applicable to low impact BES Cyber Systems.

LEGEND
Action is probably not required
Action may be required
Action is required by 1/1/2020

CIP Requirements Applicable to Low Impact BES Cyber Systems

Present Standard/Requirement	Effective Date	Retirement Date	New Standard/Requirement	Effective Date	New Description	Change Summary CIP-003-6 to CIP-003-7
CIP-002-5.1 R1	7/1/2016				BES Cyber System identification	No Change
CIP-002-5.1 R1 Part 1.3	7/1/2016				Low impact BES Cyber System identification (asset level)	No Change
CIP-003-6 R1	7/1/2016	12/31/2019	CIP-003-7 R1	1/1/2020	Cyber Security Policy	No Change
CIP-003-6 R1 Part 1.1	7/1/2016	12/31/2019	CIP-003-7 R1 Part 1.1	1/1/2020	Policy for high/medium impact BES Cyber Systems	No Change
CIP-003-6 R1 Part 1.2	4/1/2017	12/31/2019	CIP-003-7 R1 Part 1.2	1/1/2020	Policy for low impact BES Cyber Systems	Added two new policy sections
CIP-003-6 R1 Part 1.2.1	4/1/2017	12/31/2019	CIP-003-7 R1 Part 1.2.1	1/1/2020	Policy for low impact BES Cyber Systems - Cyber Security Awareness	No Change
CIP-003-6 R1 Part 1.2.2	4/1/2017	12/31/2019	CIP-003-7 R1 Part 1.2.2	1/1/2020	Policy for low impact BES Cyber Systems - Physical Security Controls	See Text
CIP-003-6 R1 Part 1.2.3	4/1/2017	12/31/2019	CIP-003-7 R1 Part 1.2.3	1/1/2020	Policy for low impact BES Cyber Systems - Electronic access controls	Removed language regarding LERC and Dial-up Connectivity
CIP-003-6 R1 Part 1.2.4	4/1/2017	12/31/2019	CIP-003-7 R1 Part 1.2.4	1/1/2020	Policy for low impact BES Cyber Systems - Cyber Security Incident response	References to ES-ISAC should be changed to E-ISAC
			CIP-003-7 R1 Part 1.2.5	1/1/2020	Policy for low impact BES Cyber Systems - Transient Cyber Assets and Removable Media malicious code risk mitigation	New policy section covering TCAs
			CIP-003-7 R1 Part 1.2.6	1/1/2020	Policy for low impact BES Cyber Systems - Declaring and responding to CIP Exceptional Circumstances	New policy section covering CIP Exceptional Circumstances
CIP-003-6 R2	4/1/2017	12/31/2019	CIP-003-7 R2	1/1/2020	Calls Attachment 1 into scope for low impact BES Cyber Systems	No Change
CIP-003-6 Att 1 Section 1	4/1/2017	12/31/2019	CIP-003-7 Att 1 Section 1	1/1/2020	Security awareness	No Change
CIP-003-6 Att 1 Section 2	None		CIP-003-7 Att 1 Section 2	1/1/2020	Physical access controls	See Text
CIP-003-6 Att 1 Section 3	None		CIP-003-7 Att 1 Section 3	1/1/2020	Electronic access controls	See Text
CIP-003-6 Att 1 Section 4	4/1/2017	12/31/2019	CIP-003-7 Att 1 Section 4	1/1/2020	Cyber Security Incident response plan	Changed ES-ISAC to E-ISAC
			CIP-003-7 Att 1 Section 5	1/1/2020	Transient Cyber Assets	See Text
CIP-003-6 R3	7/1/2016	12/31/2019	CIP-003-7 R3	1/1/2020	Designation of CIP Senior Manager	No Change
CIP-003-6 R4	7/1/2016	12/31/2019	CIP-003-7 R4	1/1/2020	CIP Senior Manager delegations	No Change
CIP-004-6 to CIP-011-2	7/1/2016				Not applicable to low impact BES Cyber Systems	Not Applicable
CIP-012-1	TBD				Control Center communications - under development - ballot open	To Be Determined
CIP-013-1	TBD				Not applicable to low impact BES Cyber Systems	Not Applicable
CIP-014-2	10/2/2015				Physical security	No Change

By: MISO

MISO's Market System Enhancement Project

Overview:

As MISO has grown over the years, so have the demands and requirements of MISO's market systems. The current system has served MISO and its members well but requires an upgrade to meet long-term needs as our industry evolves.

To ensure MISO is ready to meet the challenges and opportunities of the future, MISO's Market System Enhancement (MSE) program is transforming the current platform into a flexible, upgradeable, and secure system that ensures value, reliability and security for stakeholders.

The program moves MISO closer to fulfilling the organization's vision of being the most reliable, value-creating RTO.

Program Elements: Extend, Design, and Upgrade

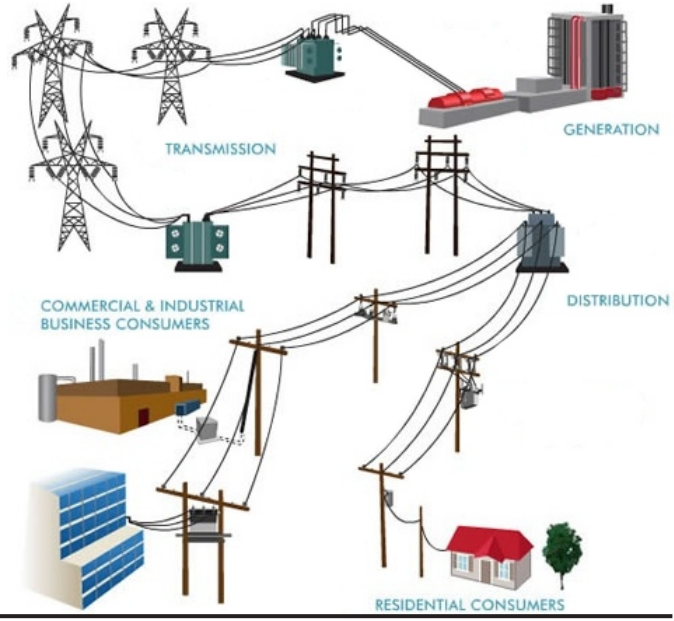
In 2017, an evaluation of MISO's existing market systems found that the current system is unable to meet long-term needs and requirements, confirming that it was time to plan and build a system of the future. Over a seven-year period, MISO's MSE team will extend the life of the current market system platform, design the platform of the future, and upgrade the platform so it is adaptable and offers transformative market opportunities.

Incremental investments will extend the life of the current system in order to continue meeting near-term requirements until a new system is fully in place. Additionally, the MSE team is conducting in-depth analysis of the current system and anticipated future needs to generate requirements for the new system.

Over the next two years, MISO will continue laying the groundwork for the new market system. While designing the new market system platform, the MSE team will establish the technical foundation by building upon capabilities to leverage key data for markets and reliability systems. During this phase, MISO will continue evaluating technology, processes, and vendors in case there is a need to make further modifications due to performance concerns or changing business requirements.

In 2019, MISO will confirm the final design of the new system and the MSE team will begin building MISO's enhanced market system. The new market system will be fully integrated in 2024.

The new market system will operate in modular, adaptable, and extensible capacities to offer maximum value to stakeholders and meet evolving needs in the long-term. The MSE program plays a critical role in executing MISO's mission and fulfilling its vision in being the most reliable, value-creating RTO. This initiative to enhance its market system platform not only recognizes the upcoming end-of-life of the current market system, but it also responds to MISO's organizational values in enhancing value to stakeholders and ensuring the future reliability of the grid.



The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

Low Impact Update

In this recurring column, I explore various CIP issues. I share with you my views and opinions, which are not binding, but rather are intended to provoke discussion within your entity and to be helpful to you as you and your entity strive to improve your compliance posture and work toward continuous improvement in the reliability, security, resiliency, and sustainability of your CIP compliance programs. There are times that I may also discuss areas of the standards that other entities may be struggling with and share my ideas to overcome their known issues. As with lighthouses, I can't steer your ship for you, but perhaps I can help shed light on the sometimes stormy waters of CIP compliance.

On April 19, 2018, FERC issued Order 843 approving CIP-003-7, Security Management Controls. See the article on pages 11 and 12 of this Newsletter for details. In recognition of this action, I'll explore multiple questions related to low impact BES Cyber Systems.

Physical and Electronic Access Controls Implementation Date

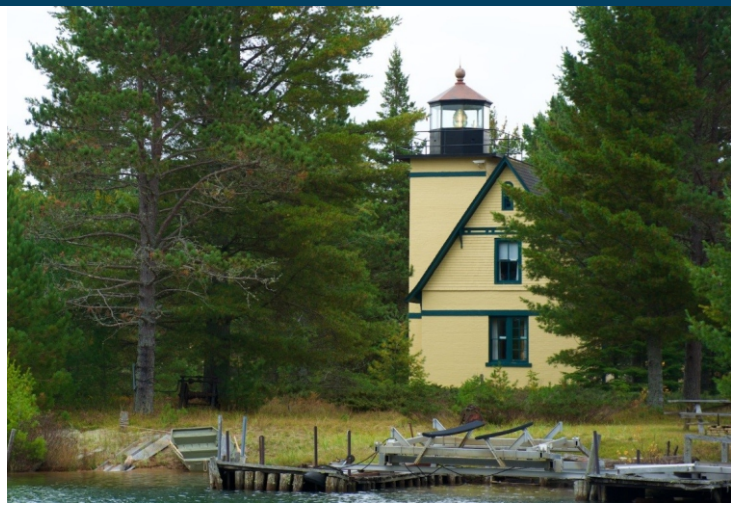
Q With FERC approving CIP-003-7, do I still need to put physical and electronic access controls in place for my low impact BES Cyber Systems by September 1st of this year?

A No. Neither the physical access controls of CIP-003-6 Attachment 1 Section 2 nor the electronic access controls of CIP-003-6 Attachment 1 Section 3 will go into effect. Instead, these controls have been replaced by CIP-003-7 Attachment 1 Sections 2 and 3, with an effective date of January 1, 2020. You have an extra 16 months to put these controls in place. However, I recommend that you do not interrupt or postpone your efforts to bring your assets with low impact BES Cyber Systems into compliance. Instead, use this gift of time to put your controls in place and test them thoroughly. You can test different approaches and see what works (and what doesn't) without a compliance risk. You can also use this time to mature these controls so that they are an integral part of your operations, similar to a pre-job safety briefing.

FERC-ordered Study of Electronic Access Controls

Q Why did FERC order a study to assess the implementation of CIP-003-7?

A Without asking the Commission directly, we can't know for sure. But we can make some inferences based on the public documents available.



Mandan, MI - Photo: L. Folkerth

In its Notice of Proposed Rulemaking (NOPR) for CIP-003-7, FERC expressed concern that CIP-003-7 Attachment 1 Section 3.1 "does not appear to contain clear criteria or objective measures to determine whether the electronic access control strategy chosen by the [R]esponsible [E]ntity would be effective for a given low impact BES Cyber System to permit only necessary inbound and outbound connections" (NOPR, P. 29). In particular, I believe FERC was concerned about the phrase "as determined by the Responsible Entity" (NOPR, P. 24-26) and about a lack of objective measures to assess compliance (NOPR, P. 28-29).

Instead of ordering more stringent language in Section 3, FERC was persuaded to let industry implement the existing language (Order 843, P. 27-30). FERC also established several very clear expectations:

- Responsible Entities are expected to be able to provide a technically sound explanation as to how the electronic access controls meet the security objective.
- NERC and the Regional Entities will have the ability to assess the effectiveness of the electronic access control plan required by CIP-003-7 R2.
- NERC and the Regional Entities will have the ability to assess an entity's adherence to its electronic access control plan.

In order to verify that these expectations are being met, NERC is required to perform the study you asked about. The study will include:

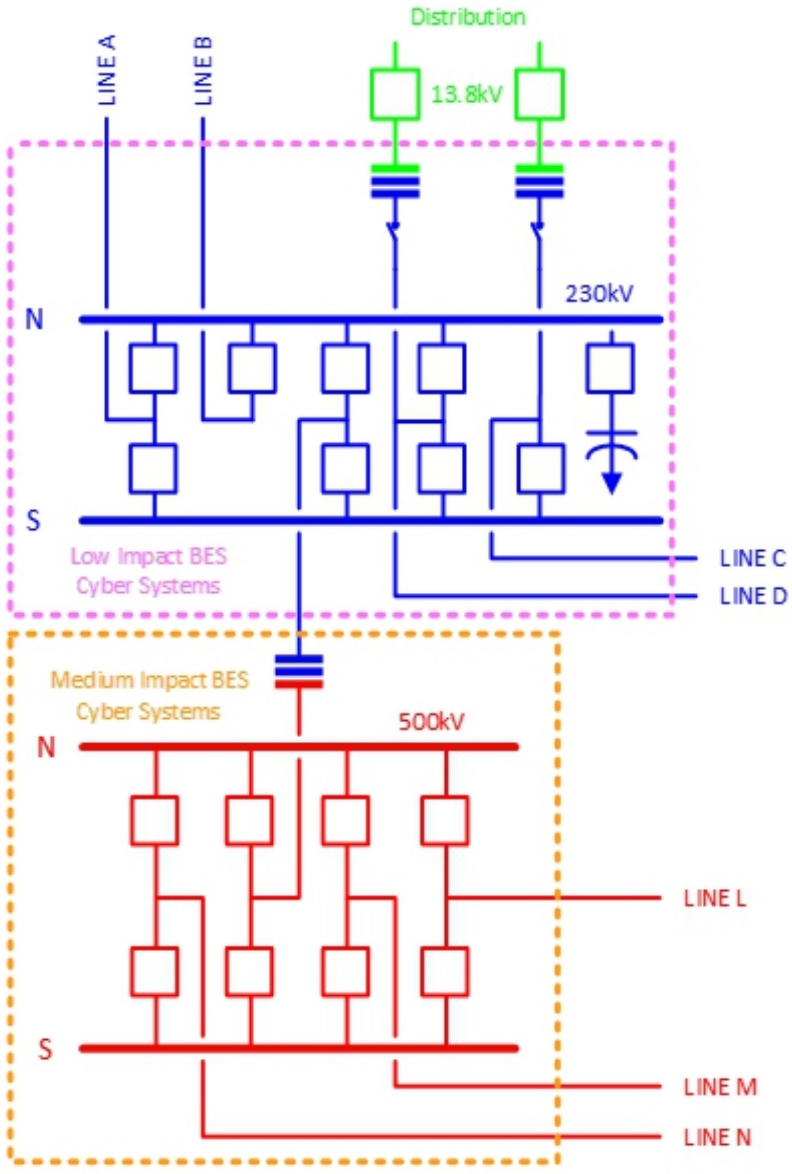
- What electronic access controls entities choose to implement;
- Under what circumstances these controls are implemented;
- The adequacy of these controls; and
- Other relevant information.

When audits of your electronic access controls for low impact BES Cyber Systems

Continued on page 15

Continued from page 14

Figure 1



begin in 2020, you should expect them to be very detailed and thorough. The audit teams will not only be reviewing your compliance with the Standard and its associated controls, they will be gathering information to provide to NERC for its study.

Impact of IRC 2.4 on Low Impact BES Cyber Systems

Q Does the presence of 500kV or above bring an entire substation up to medium impact?

A No, not by itself. According to CIP-002-5.1a Attachment 1 Impact Rating Criterion (IRC) 2.4, BES Cyber Systems associated with substation Facilities operating at 500kV or more will be assigned a medium impact rating. Note the capital "F" of Facilities calls out the Glossary definition, "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)" These Facilities will include any transformer with a high side at 500kV or more, and breakers, reactors, capacitors, etc. operating at 500kV or more.

However, BES Cyber Systems associated with the remaining Facilities within the substation will be evaluated according to IRC 2.5. IRC 2.5 contains two criteria. In order to meet IRC 2.5, a substation must connect at 200kV or higher to three other substations. If this is true, then an aggregate weighted value is calculated based on the number of lines crossing the substation boundary and the voltage level of those lines. If this aggregate weighted value exceeds 3000, then the BES Cyber Systems associated with Facilities at that substation receive a medium impact rating. Otherwise, those BES Cyber Systems receive a low impact rating per IRC 3.2.

For example, the substation in Figure 1 connects to seven other substations by 230kV and 500kV lines. Each line is protected by breakers. There is a capacitor on the 230kV side of the transformer. BES Cyber Systems associated with the 230kV/500kV transformer and the 500kV breakers will have a medium impact rating. Since the substation is connected to three or more other substations at voltages above 200kV, we need to calculate the aggregate weighted value of the substation. We do The aggregate weighted value for this substation does not exceed 3000. Therefore the BES Cyber

Line	Line Voltage	Line Weight Value
A	230kV	700
B	230kV	700
C	230kV	700
D	230kV	700
L	500kV	0
M	500kV	0
N	500kV	0
Distribution	13.8kV	Out of Scope
Aggregate Weighted Value		2800

Systems associated with the 230kV breakers and the 230kV capacitor will be assigned a low impact rating.

List of Low Impact BES Cyber Systems

Q Is a list of low impact BES Cyber Systems required?

A Based on the notes attached to CIP-002-5.1a R1 and CIP-003-7 R2, the audit teams cannot require a list of low impact BES Cyber Systems at an asset. If we take a close look at CIP-003-7 Attachment 1 Section 3, however, we see

Continued on page 16

Continued from page 15

that electronic access controls are required for any routable communications that are between a low impact BES Cyber System and a Cyber Asset outside the asset containing low impact BES Cyber Systems. If you take the approach that any routable communications crossing the asset boundary may originate or terminate at a low impact BES Cyber System, and control electronic access accordingly, then you will not need to identify individual BES Cyber Systems, but only the assets containing low impact BES Cyber Systems.

At a generator or substation, you have the flexibility within the language of the Standard to say that not all communications are to low impact BES Cyber Systems. In order to take advantage of this flexibility you need to know which Cyber Assets are members of low impact BES Cyber Systems so that you can control electronic access to those Cyber Assets. You must be able to provide sufficient, appropriate evidence that you are protecting communications to low impact BES Cyber Systems. In order to provide this evidence you will need to know, and provide evidence regarding, which Cyber Assets are part of a low impact BES Cyber System and which are not.

One way of thinking of this is to differentiate whether you provide low impact protections at the asset (substation or generator) level or at the BES Cyber System level. If protections are at the BES Cyber System level, then you will need to be able to identify the Cyber Assets being protected. There are several places within CIP-003-7 Attachment 1 that permit compliance at the BES Cyber System level:

- Section 2, Physical security controls, permits an entity to control access to the locations of the low impact BES Cyber Systems at the asset;
- Section 3, Electronic access controls, permits an entity to control electronic access to a low impact BES Cyber System; and
- Section 5, Transient Cyber Asset and Removable Media malicious code risk mitigation, requires mitigation of the threat of the introduction of malicious code to low impact BES Cyber Systems.

In each of these cases, if you treat all Cyber Assets at an asset as low impact BES Cyber Systems, then you will not need to identify individual BES Cyber Systems to your audit team. However, if the Cyber Assets at an asset are treated differently based on whether they are members of a low impact BES Cyber System, then you will need to be able to identify those systems are that are required to be protected.

Initial Test of Incident Response Plan

Q Does the approval of CIP-003-7 alter the required date for the first test of my Cyber Security Incident response plan for low impact BES Cyber Systems?

A No, the first test of your incident response plan was due on April 1, 2017. This is not changed by CIP-003-7.

The CIP-003-5 Implementation Plan (available here) on page 2 states that the initial performance of periodic requirements in CIP-003-5 R2 is the effective date of CIP-003-5 R2, which was April 1, 2017. The CIP-003-6 Implementation Plan (available here), on page 10, incorporates the CIP-003-5 Implementation Plan by reference.

The CIP-003-7 Implementation Plan (available here) states, "The effective dates or phased-in compliance dates within the CIP-003-6 Implementation Plan, remain in effect except that the compliance dates for CIP-003-6, Requirement R2, Attachment 1, Sections 2 and 3 shall be replaced with the effective date of CIP-003-7."

This makes it clear that the compliance dates for Section 4 do not change with CIP-003-7's approval.

If you did not understand this and have yet tested your low impact Cyber Security incident response plan, I strongly recommend that you perform a test as soon as practical. You should also contact the RF Enforcement Group to discuss and work through any potential noncompliance.

I also recommend testing your plan much more frequently than the Standard requires. It is important for even low impact BES Cyber Systems to have a usable and effective Cyber Security Incident response plan, and to have a trained and proficient incident response team to carry out the plan.

Requests for Assistance

If you are an entity registered within RF and believe you need assistance in sorting your way through this or any compliance related issue, remember RF has the Assist Visit program. Submit an Assist Visit Request via the rfirst.org web site here.

Feedback

Please share any feedback you may have on these articles. Suggestions for topics are always appreciated.

I may be reached here.

Regulatory Affairs

House and Energy Committee Approves Cybersecurity, Natural Gas Legislation

On May 9, 2018, the House Energy and Commerce Committee approved a comprehensive piece of energy legislation. The series of bills will help to secure the U.S. energy infrastructure from cyber-attacks and strengthen the DOE's cybersecurity preparedness.

The first bill, the Pipeline and LNG Facility Cybersecurity Preparedness Act (H.R. 5175), will require the Secretary of Energy to carry out a program among federal agencies, states, and the energy industry to protect the security of natural gas pipelines, hazardous liquid pipelines, and LNG facilities.

The second bill, the Enhancing Grid Security through Public-Private Partnerships Act (H.R. 5240), will establish a voluntary DOE "Cyber Sense" program to test the cybersecurity of products and technologies that may be used in the bulk power system and grant the DOE permission to provide technical assistance to utilities and various stakeholders to mitigate cyber security vulnerabilities.

The third bill, the Cyber Sense Act of 2018 (H.R. 5239), will develop a program within the DOE to facilitate public-private partnerships to enhance cybersecurity for rural or smaller entities.

This program requires a report to Congress assessing threats, vulnerabilities, and a cost-benefit analysis of the implementation of related actions.

NERC Files Comments to FERC on Resilience

On May 9, 2018, NERC filed comments supporting resilience of the BPS in response to FERC's proceeding to evaluate the resilience of the BPS in regions operated by Regional Transmission Organizations and Independent System Operators (collectively, RTOs). FERC's proceeding seeks to (1) develop a common understanding of the term resilience; (2) understand how RTOs assess resilience; and (3) evaluate whether additional FERC action is appropriate.

NERC's comments discuss how resilience is a component of reliability in relation to an event and thus is a key part of NERC's mission and activities. NERC's comments also highlight how NERC Reliability Standards and other activities help support resilience and emphasize how it is important to reexamine resilience in light of the changing generation resource mix across the ERO and evolving cyber and physical security threats. NERC's full comments to FERC can be read here.

E-ISAC Expands Industry Engagement Program

The NERC Electricity Information Sharing and Analysis Center, in collaboration with the Large Public Power Council, began an Industry Augmentation Program initiative to improve cooperation and information sharing. It involves member utilities hosting multi-day visits to work alongside E-ISAC personnel to provide insight into the needs of both organizations, raise awareness, and increase feedback opportunities to strengthen security efforts across North America.

Since January, eight utilities have participated in the augmentation program, including cyber security experts from publicly owned utilities and investor-owned utilities.

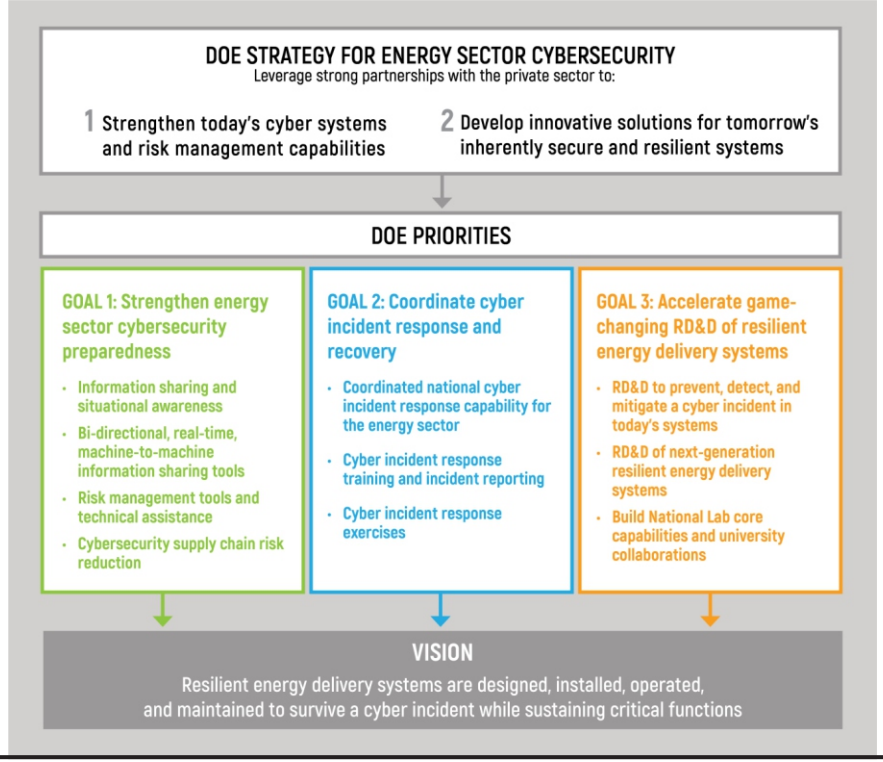
Regulatory Affairs

The Department of Energy's Innovative Approach to Changing the Future of Cyber Security

In response to an ever increasing amount of cyber threats and cyber-attacks, the Department of Energy ("DOE") announced its new Multiyear Plan for Energy Sector Cybersecurity on May 14, 2018. This five year plan will focus on three priorities: strengthening preparedness, coordinating responses, and developing the next generation of resilient energy systems.

Given the reality that cyber threats continue to outpace industry's best defenses, DOE determined that it needed to pursue disruptive changes in its cyber risk management practices. The DOE's strategy is to strengthen today's energy delivery systems to address emerging threats and to develop game-changing solutions that will create secure and resilient energy systems. The Multiyear Plan has three main goals, outlined in the graphic below.

The full Multiyear Plan is available here.



FERC issues final rule on Revised CIP Security Management Controls Standard

Last month, FERC finalized revisions to CIP-003-7 (Cyber Security-Security Management Controls) in response to a FERC NOPR issued in October. The Standard aims to prevent malware from infecting low-impact computer systems through transient electronic devices such as laptops and thumb drives.

The proposed modifications are expected to improve the base-line cybersecurity stance for responsible entities.

Modifications began in January 2016 under Order No. 822 in which FERC directed NERC to eliminate ambiguity on the term "direct" and to modify CIP Standards for mandatory protection for transient electronic devices used at low impact BES Systems.

The October 2017 NOPR ordered NERC to explicitly address the need to mitigate potentially malicious code from third-party transient devices within the Standard.

In the final rule, FERC declined a proposal to clarify criteria for electronic access controls for low impact systems as the current Standard sufficiently establishes compliance expectations.

Instead, FERC directed NERC to further assess the criteria when modifying the Standard.

In the Industry

DER Technical Conference Expands Upon FERC NOPR, Report

On April 10-11, industry experts convened for a Distributed Energy Resources (DER) Technical Conference to help FERC Commissioners determine actions to take on DER aggregation reforms included in their Notice of Proposed Rulemaking (NOPR) on Electric Storage Participation in Markets Operated by RTO's and ISO's. Panelists also discussed issues related to potential DER effects on the Bulk Power System.

The NOPR ordered RTOs and ISOs to remove participation barriers for electric storage resources in capacity, energy, and ancillary services markets as current market rules create barriers for entry in emerging technologies. FERC released an earlier report discussing potential reliability concerns for the BPS if increases in DER capacity are not adequately accounted for and executed. The report determined that further discussion was needed to improve and refine data available and incorporate it into planning and operating models.

The first day of the conference focused on

- Economic Dispatch, Pricing, and Settlement of DER Aggregations;
- Operational Implications of DER Aggregation with State and Local Regulators; and
- Participation of DERs in RTO/ISO Markets.

Panelists addressed the option for states to decide on retail or wholesale energy as well as concerns about new products being signed off on by utilities and states before entering the market. Concerns included the potential to affect reliability if the signing off process is not transparent and limited.

On the second day, panelists discussed

- the Collection and Availability of Data on DER Installations;
- Incorporating DERs in Modeling;
- Planning and Operations Studies;
- Coordination of DER Aggregations Participating in ISO/RTO Markets; and
- Ongoing Operational Coordination.

PJM and MISO shared their data sharing processes and avenues into wholesale markets for DERs. Discussions were also around issues regarding the roles of utilities, grid infrastructure, coordination frameworks, and operational challenges.

PJM Announces Next Phase of Grid Resilience Initiative

PJM Interconnection introduced the next steps in its initiative to safeguard future fuel security for electricity generation on its power system serving 65 million people. Fuel security is critical for resilience, as public policies, lower fuel prices and technology improvements continue to alter the traditional mix of generation resources.

PJM will initiate a process analyzing fuel security vulnerabilities and create criteria to evaluate areas in the PJM system that could face fuel security issues in the future.

PJM will:

(1) Identify system vulnerabilities and characteristics such as on-site fuel requirements, dual-fuel capability or others that ensure that peak demands can be met during extreme scenarios;

(2) Model those vulnerabilities as constraints in PJM's capacity market, allowing for valuation of required attributes in the market; and

(3) Continue to work with the U.S. Department of Homeland Security, the U.S. Department of Energy, the Federal Energy Regulatory Commission, states, stakeholders and others to guarantee that the results are consistent with identified security needs in the PJM footprint, including service to vital military installations and other identified security concerns.

Standards Update

This recurring column provides our Registered Entities with relevant and recent updates to the Reliability Standards and Requirements.

General NERC Standards News

Updated FAQ on Implementation Plans for PRC-026-1 Posted

The FAQ document provides various scenarios to assist the Generator Owner, Transmission Owner, and Planning Coordinator in understanding the Reliability Standard PRC-026-1 – Protection System Response to Stable Power Swings Implementation Plan. The updated version includes a date correction from 9/1/2020 to 9/1/2021 to R3 in the center column.

2018 Registered Ballot Body Self-Select Attestation Process Beginning Soon

Appendix 3D Registered Ballot Body Criteria of Procedure states:

'Each participant, when initially registering to join the Registered Ballot Body (RBB), and annually thereafter, shall self-select to belong to one of the Segments…'

NERC Standards staff will be initiating the 2018 Annual RBB Self-Select Process in the coming weeks.

- May 2018 – Each RBB voting member will receive a notification with a link to the SBS (an electronic) attestation page confirming that there have been no material changes in the last 12 months that affect the entity's current Segment selection(s), thus the entity continues to meet the Segment qualifications (as outlined in the qualifications in Appendix 3D: RBB Criteria referenced above).
- June 2018 – Deadline for all RBB members to self-select their segments via the SBS.

Notifications will be sent via RBB email, Standards Committee communications, Standards, Compliance, and Enforcement Bulletins, and other NERC email alerts. Specific dates to be determined. For more information or assistance, contact Wendy Muller.

NERC Reliability Standard EOP-004-4 Better Aligned with Department of Energy's OE-417 Form

Through an extensive collaborative process, a better alignment to reportable events in Attachments 1 and 2 of EOP-004-4 (approved by FERC January 18, 2018) with the DOE's OE-417 (current version became effective April 1, 2018), was developed to gain efficiency by eliminating redundant reporting of a single event to multiple entities. The new version of DOE's OE-417 is currently in effect, while EOP-004-4 is subject to future enforcement.

It is important to note that entities will be required to report all events as required under EOP-004. For U.S. entities, if an event is required to be reported to DOE under the OE-417 form – and – that same event is required to be reported to NERC under EOP-004-3 (currently enforced), then subsequently EOP-004-4 (subject to future enforcement), NERC will accept the OE-417 submission in lieu of EOP-004, Attachment 2. However, if the facts of the event are such that the event is required to be reported on either the OE-417 or EOP-004, Attachment 2, but not both, then the entity should report only to the single agency requiring it for the facts of the event.

For additional information on EOP-004-4, please see the slide presentation and streaming webinar.

Resources Posted

NERC has posted the streaming webinar and slide presentation for the March 14, 2018 Supply Chain Risk Management webinar.

NERC has posted the streaming webinar and slide presentation for the March 22, 2018 Project 2015-10 – Single Points of Failure webinar.

NERC has also posted the streaming webinar and slide presentation for the March 26, 2018 Technical Rationale for Reliability Standards webinar.

Three New RSAWs Posted

NERC posed three new Reliability Standard Audit Worksheets (RSAWs):

- BAL-003-1.1
- INT-004-3.1
- CIP-002-5.1a
- INT-009-2.1
- INT-010-2.1

These resources can be found on NERC's RSAW page under the heading "Current RSAWs for Use."

Notable NERC Filings

In March, NERC filed the following:

- comments in response to a notice of proposed rulemaking in Docket No. RM17-13-000; an informational filing regarding the implementation of Reliability Standard TPL-001-4 Table 1, Footnote 12 in Docket Nos. RM12-1-000 and RM13-9-000;
- the 2018 NERC Standards Report, status and timetable for addressing regulatory directives in Docket No. RR09-6-003;
- a joint petition with WECC for approval of proposed Regional Reliability Standard FAC-501-WECC-2;
- a petition for approval of proposed Reliability Standard PRC-025-2 – Generator Relay Loadability; and,
- a petition for approval of the amended Compliance and Certification Committee Charter.

In April, NERC filed the following:

- its revised work plan to conduct research on topics related to geomagnetic disturbances (GMD) and their impacts on the reliability of the bulk power system.

Standards Update

Recent and Upcoming Standards Enforcement Dates

July 1, 2018

- CIP-009-6 Cyber Security Recovery Plans for BES Cyber Systems (Requirement 2.3)
- CIP-010-2 Cyber Security Configuration Change Management and Vulnerability Assessments (Requirements 3.2, 3.2.1, 3.2.2)
- MOD-026-1 Verification of Models and Data for Generator Excitation Control System or Plant Volt/Var Control Functions (Requirements R2, 2.12.1.6)
- MOD-027-1 Verification of Models and Data for Turbine/Governor and Load Control or Active Power/Frequency Control Functions (Requirements R2, 2.1-2.1.5)
- TOP-001-4 Transmission Operations
- TPL-007-1 Transmission System Planned Performance for Geomagnetic Disturbance Events (Requirement 2)

January 1, 2019

- BAL-005-1 Balancing Authority Control
- FAC-001-3 Facility Interconnection Requirements
- TPL-007-1 Transmission System Planned Performance for Geomagnetic Disturbance Events (Requirement 5)

April 1, 2019

- EOP-004-4 – Event Reporting
- EOP-005-3 – System Restoration from Blackstart Resources
- EOP-006-3 – System Restoration Coordination
- EOP-008-2 – Loss of Control Center Functionality

January 1, 2020

- CIP-003-6 – Cyber Security – Security Management Controls (Requirement 2, Att. 1, Sec. 2 and 3);
- PRC-026-1 Relay Performance During Stable Power Swings (Requirements 2-4)

July 1, 2020

- PRC-002-2 – Disturbance Monitoring and Reporting Requirements (50% compliance for Requirements 2–4, 6–11)

January 1, 2021

- PRC-012-2 – Remedial Action Schemes
- TPL-007-1 – Transmission System Planned Performance for Geomagnetic Disturbance Events (Requirement 6, 6.1-6.4)

January 1, 2022

- TPL-007-1 – Transmission System Planned Performance for Geomagnetic Disturbance Events (Requirements 3,4,7)

July 1, 2022

- PRC-002-2 – Disturbance Monitoring and Reporting Requirements (Requirements 2–4, 6–11)

More information on these and other upcoming Standards is available here.

New Standards Projects

Several new Standards projects and new project phases are underway. Projects are described on the NERC Standards website, along with links to all drafts, voting results, and similar materials. Recent additions include the following projects:

Other Active Comment Periods

Comment Period Open for Inverter-Based Resource Performance Draft Reliability Guideline

- Submit comments via email using the comment form; 05/04/18 – 06/29/18

Notable FERC Issuances

On May 2, 2018, FERC issued a letter order approving NERC's March 16, 2018 filing of proposed Reliability Standard PRC-025-2 – Generator Relay Loadability, the associated implementation plan, and the associated violation risk factors and violation severity levels.

On May 4, 2018, FERC issued a delegated letter order accepting NERC, MRO, and SERC's March 2018 joint petition requesting certain FERC approvals in connection with the dissolution of the SPP RE and the transfer of registered entities within the SPP RE footprint to MRO and SERC.

On April 13, 2018, FERC issued a delegated order granting rehearings for further consideration of FERC's Order No. 842 on Essential Reliability Services and the Evolving Bulk-Power System – Primary Frequency Response, issued on February 15, 2018.

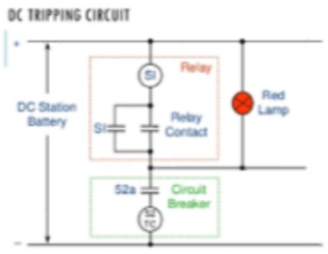
Watt's Up at RF

Protection System Workshop
August 14-15, 2018
Cleveland, OH

Click here for the Agenda and Registration

The RF Reliability Assessment and Performance Analysis (RAPA) group will host its fourth annual Protection System Workshop for technical personnel. The focus this year will be on "Protection System Drawings – the Big Picture." This is a highly interactive event with attendees providing ideas, suggestions, and stories for the benefit of everyone. There is no fee to attend this workshop and it is open to anyone interested. The final agenda will be released soon, but current topics include:

- Document Control on Multiphase Projects
- Innovate Test Twitch Designs for Safety and Reliability
- Substation Upgrade Project - When Good Drawings Go Bad
- Sharing Drawings Between Neighboring Companies



Intended Audience

- Substation designers, drafters, electricians, supervisors, field engineers
- Relay technicians, engineers and others who work directly with this equipment
- Company trainers for this subject

August 14	August 15
12:00 p.m. - 1:00 p.m. – Registration and Lunch	7:00 a.m. - 8:00 a.m. – Breakfast
1:00 p.m. - 5:00 p.m. – Workshop	8:00 a.m. - 12:00 p.m. – Workshop
5:00 p.m. - 7: 00 p.m. – Networking Reception	

Human Performance Workshop
August 15-16, 2018
Cleveland, OH

Click here for the Agenda and Registration

RF is sponsoring a one-day human performance workshop for technical personnel on August 15 and 16, 2018 at our office in Cleveland, OH.

This workshop will focus on the practical application of human performance techniques and concepts for front-line activities that attendees can take back and use in transmission reliability related work areas, such as operations, asset management, design, protection, and maintenance. This workshop will be held immediately after our annual Protection Systems Workshop for Technical Personnel.

Should you have any questions, they may be directed to Jeff Mitchell. There is no fee to attend this workshop and it is open to neighboring Regional Entity staff, members, and others.

Intended Audience

Individuals whose work focuses onfront-line activities in reliability related work areas, such as:

- Substation and transmission maintenance
- Protection and controls
- Operations control rooms including tools support personnel for EMS, SCADA, etc.
- Asset design groups (substation, transmission)
- Asset management groups
- Others interested in these topics (e.g., trainers)

August 15	August 16
11:30 a.m. - 1:00 p.m. – Registration and Lunch	7:00 a.m. - 8:00 a.m. – Breakfast
1:00 p.m. - 5:00 p.m. – Workshop	8:00 a.m. - 12:00 p.m. – Workshop
5:00 p.m. - 6:30 p.m. – Networking Reception	

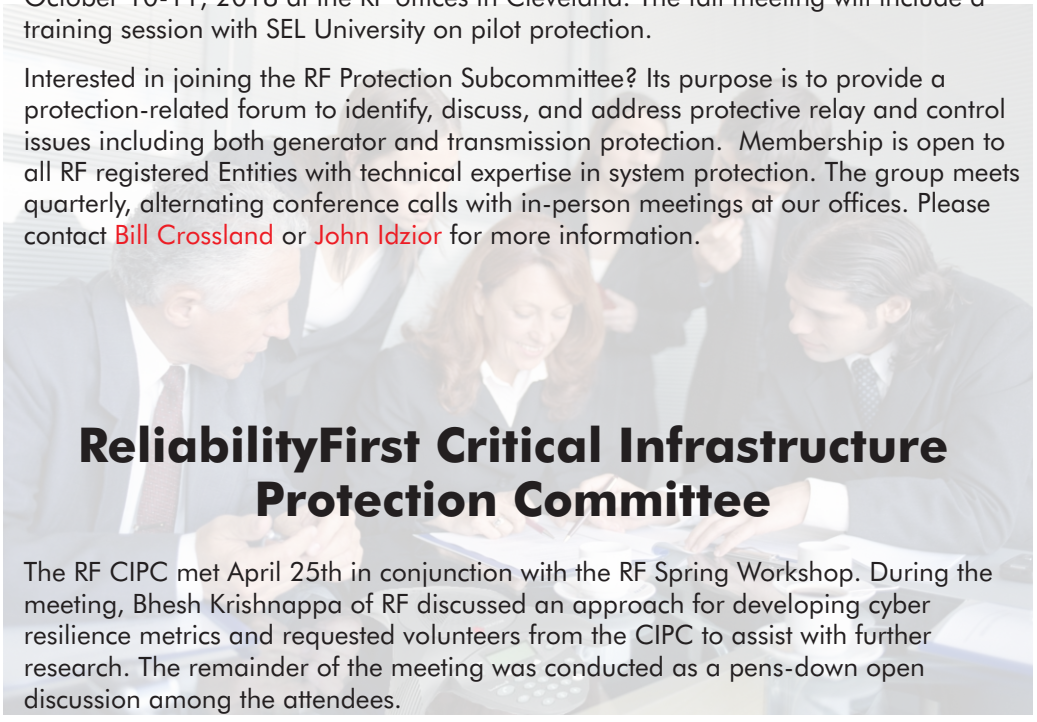
RF Protection Subcommittee

The Protection Subcommittee held its Spring meeting at the RF offices on April 4-5, 2018. They reviewed misoperation metrics for 2017 and the latest enhancements to and reporting procedures for the Misoperation Information Data Analysis System (MIDAS). The group discussed when to report misoperations and operations under different scenarios.

In addition to excellent entity participation, we were pleased to have NERC in attendance to provide an overview of the analysis performed by the Inverter-Based Resource Performance Task Force, which was formed in response to loss of generation events in the Western Interconnection in 2017.

Future discussions will delve into the 2019 short circuit coordination effort, and the group's next meetings will be a conference call on July 11, 2018 and a meeting on October 10-11, 2018 at the RF offices in Cleveland. The fall meeting will include a training session with SEL University on pilot protection.

Interested in joining the RF Protection Subcommittee? Its purpose is to provide a protection-related forum to identify, discuss, and address protective relay and control issues including both generator and transmission protection. Membership is open to all RF registered Entities with technical expertise in system protection. The group meets quarterly, alternating conference calls with in-person meetings at our offices. Please contact Bill Crossland or John Idzior for more information.



ReliabilityFirst Critical Infrastructure Protection Committee

The RF CIPC met April 25th in conjunction with the RF Spring Workshop. During the meeting, Bhesh Krishnappa of RF discussed an approach for developing cyber resilience metrics and requested volunteers from the CIPC to assist with further research. The remainder of the meeting was conducted as a pens-down open discussion among the attendees.

Entity Profile Questionnaire Tool

As you may be aware, RF is rolling out a new Entity Profile Questionnaire (EPQ) tool to collect data and information to evaluate and understand the potential impact that each Entity may have on the Bulk Electric System. This information will help us make our Compliance Monitoring and Enforcement Program activities more efficient and effective.

The focus of the collection is based on your Entity's organizational makeup, technical information, compliance history, culture, overall Entity performance, industry trends, and numerous attributes and qualities of your compliance program.

So far, RF has rolled out the EPQ to 113 Entities (almost half of the total RF Entities) and we really appreciate those entities who have spent time working with us thus far to ensure our information is complete, current and accurate. RF will be rolling out the fourth batch of entities by early August.

To those who have not received a request yet, we look forward to working with you this year. We are confident the time invested now will save us both time later while helping improve reliability.

Our process is to issue a request and collect the information with a secure tool, called MKInisght. In conjunction with the rollout we are providing training and educational webinars. However, if you have any questions or concerns about this process, please reach out to us here.

Monthly Reliability and Compliance Forum Call

The next Monthly Reliability and Compliance Forum Call will occur on Monday, June 18, 2018 at 2 p.m. EST. The topics slated for discussion on the June call include: an overview of our Entity Profile Tool and a recap of our Guided Self-Certification Process. Dial-in information is available in the Monthly Reliability and Compliance Forum Call announcement on the Compliance page of the RF website. Please contact Jim Uhrin with any questions, suggestions, or topics of interest you have for future calls.

Calendar of Events

Complete calendar of RF Upcoming Events is located on our Website:

Date	RF Upcoming Events	Location
June 18	Reliability and Compliance Open Forum Call	Conference Call
June 27-28	CIPC Meeting	Milwaukee, WI
June 28	EMS Working Group	WebEx
July 16	Reliability and Compliance Open Forum Call	Conference Call
July 26	EMS Working Group	WebEx
August 14-15	Protection System Workshop	Cleveland, OH
August 15-16	Human Performance Workshop	Cleveland, OH
August 20	Reliability and Compliance Open Forum Call	Conference Call
August 29-30	ReliabilityFirst Board of Directors Meetings	Cleveland, OH
August 30	EMS Working Group	WebEx

Industry Events:

Date	Industry Upcoming Events
June 13	NERC Inverter-Based Resource Webinar Series - Recommended Performance for Inverter-Based Resources Connected to the Bulk Power System – NERC Reliability Guideline
June 14	BOTCC Executive Session
June 18-22	GADS Conventional and Wind Training
June 20-21	2018 Power System Modeling Conference
June 21	FERC Open Meeting
June 26-28	Technical Conference regarding Increasing Market and Planning Efficiency and Enhancing Resilience through Improved Software (Docket No. AD10-12-009) (Washington, DC) (Free Web Cast)
July 12	BOTCC Executive Session
July 19	FERC Open Meeting
July 24-25	Standards and Compliance Workshop
July 31	Reliability Technical Conference regarding the Bulk-Power System (Docket No. AD18-11-000) (Washington, DC) (Free Web Cast)
August 14	BOTCC Executive Session
August 15	BOTCC Open Meeting

SHARE YOUR FEEDBACK

Please email any ideas or suggestions for the newsletter to prcommrequest@rfirst.org

SUBSCRIBE TO THE NEWSLETTER

Click Here

Follow RF on

@RFirst_Corp

Public Service Commission of Wisconsin Issues Request for Proposal for the Inaugural Round of Energy Innovation Grant Program

On May 2, 2018, the Office of Energy Innovation, within the Public Service Commission of Wisconsin, issued a Request for Proposals in the initial round of the Energy Innovation Grant Program. The Commission expects $5 million in awards to grantees in the inaugural round of grants. The Energy Innovation Grant Program is designed to help decrease energy consumption, boost the use of renewable energy and transportation technologies, support preparedness and resiliency in the energy system, and create a more comprehensive energy plan for Wisconsin's future. Over the lifetime of the program, more than $25 million in grants will be awarded.

ReliabilityFirst Members

Forward Together RF ReliabilityFirst

AEP ENERGY PARTNERS
AES NORTH AMERICA GENERATION
ALLEGHENY ELECTRIC COOPERATIVE, INC
AMERICAN ELECTRIC POWER SERVICE CORP
AMERICAN TRANSMISSION CO, LLC
APPALACHIAN POWER COMPANY
BUCKEYE POWER INC
CALPINE ENERGY SERVICES, LP
CITY OF VINELAND, NJ
CLOVERLAND ELECTRIC COOPERATIVE
CMS ENTERPRISES COMPANY
CONSUMERS ENERGY COMPANY
DARBY ENERGY, LLP
DATACAPABLE, INC
THE DAYTON POWER & LIGHT CO
DOMINION ENERGY, INC
DTE ELECTRIC
DUKE ENERGY SHARED SERVICES INC
DUQUESNE LIGHT COMPANY
DYNEGY, INC
EDISON MISSION MARKETING AND TRADING, INC.
EXELON CORPORATION
FIRSTENERGY SERVICES COMPANY
HAZELTON GENERATION LLC
HOOSIER ENERGY RURAL ELECTRIC COOPERATIVE, INC
ILLINOIS CITIZENS UTILITY BOARD
ILLINOIS MUNICIPAL ELECTRIC AGENCY
INDIANA MUNICIPAL POWER AGENCY
INDIANAPOLIS POWER & LIGHT COMPANY
INTERNATIONAL TRANSMISSION COMPANY
LANSING BOARD OF WATER AND LIGHT
LINDEN VFT, LLC
MICHIGAN ELECTRIC TRANSMISSION CO, LLC
MICHIGAN PUBLIC POWER AGENCY
MIDCONTINENT INDEPENDENT SYSTEM OPERATOR, INC
MORGAN STANLEY CAPITAL GROUP, INC
NEPTUNE REGIONAL TRANSMISSION SYSTEM, LLC
NEXTERA ENERGY RESOURCES, LLC
NORTHERN INDIANA PUBLIC SERVICE COMPANY
OFFICE OF PEOPLE'S COUNSEL, DISTRICT OF COLUMBIA
OHIO POWER COMPANY
OHIO VALLEY ELECTRIC CORPORATION
OLD DOMINION ELECTRIC COOPERATIVE
PENNSYLVANIA OFFICE OF CONSUMER ADVOCATE
PJM INTERCONNECTION, LLC
PPL ELECTRIC UTILITIES CORPORATION
PROVEN COMPLIANCE SOLUTIONS, INC
PUBLIC SERVICE ENTERPRISE GROUP, INC
ROCKLAND ELECTRIC COMPANY
SOUTHERN MARYLAND ELECTRIC COOPERATIVE, INC
TALEN ENERGY
TENASKA, INC
TENNESSEE VALLEY AUTHORITY
UTILITY SERVICES, INC
VECTREN ENERGY DELIVERY OF INDIANA, INC
WABASH VALLEY POWER ASSOCIATION, INC
WISCONSIN ELECTRIC POWER COMPANY
WOLVERINE POWER SUPPLY COOPERATIVE, INC