Issue 3
2020 May/June

INSIDE THIS ISSUE

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

Follow us on:

Note from the President

Dear Stakeholders,

After discussing the adjustment to a "new normal" in our previous newsletter, my hope was that the toughest times of 2020 were behind us. I am still hopeful and optimistic that is the case. Many in our industry, especially control center operations teams who still may be sheltering-in-place and field personnel, have not had the luxury of transitioning to a work-from-home scenario — so I must send my continued gratitude for your dedication and sacrifices.

This year will certainly go down in history as one of immense change. Maybe even a few short years ago I would have addressed the difficult and sensitive current events with a statement like: "It goes without saying that I am against violence and racism" — but it is no longer good enough to assume that such crucial statements, especially from those in leadership positions, can "go without saying." No matter where you stand during this polarizing time in our country's history, we all must acknowledge that hate has no place here.

Each one of us plays a role in making positive changes in our world. The RF footprint is made up of all types of communities and people, and we are proud to serve each and every one of them. Our mission of preserving and enhancing the reliability and security of the BPS has always been aimed at the support and advancement of our country's public welfare. We are taking this opportunity to examine how we are fulfilling that mission statement, what it truly means, and how we can do it better.

Showing off the talent on the RF team is one of the most rewarding parts of my job, so please do not miss the article in this issue about staff accreditations. Our phased approach for returning to the office begins after 4th of July, but, in the meantime,I am incredibly proud of how well they adjusted to operating under our business continuity plan. The team has done a fantastic job of executing key activities, like board meetings and assist visits, from home. While obviously not ideal, it shows that our staff truly exemplifies the resiliency we work so hard to provide for the grid.

Another essential RF activity is our Annual Workshops. We were disappointed to have to cancel our Spring Workshop in April, but we are looking forward to hosting a webinar on Tuesday, August 25 to replace our Fall Workshop previously scheduled for September in Cleveland. This one-day session will focus on FAC-008/Reliability in the morning and Supply Chain/CIP-013 in the afternoon. Registration details will be available soon, and I hope the virtual setting allows for those of you who generally miss our workshops due to budget and resource constraints to join us.

Be safe and be well.

Forward Together,

Tim

From the Board

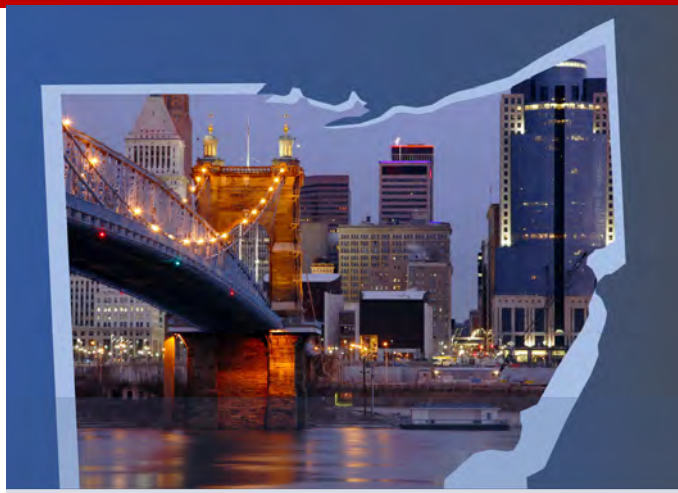
RF held its Second Quarter Board of Directors meetings via WebEx on June 3-4. RF staff and special guests provided presentations on various topics. Highlights include the following:

The keynote speaker was Teri Stasko, Assistant General Counsel and Director of Enforcement at NERC. Ms. Stasko discussed the ERO Enterprise transformation and its emphasis on teamwork, knowledge sharing, and innovative solutions. She also addressed the ERO's recent efforts related to the COVID-19 pandemic, including the issuance of guidance on tracking and processing COVID-19-related noncompliance.

Jordan Bakke, Senior Manager Policy Studies at MISO, presented MISO's Resource Availability and Need (RAN) effort and how the footprint is projected to move to 32% renewables over the next 10 years. He noted that MISO's RIIA (Renewable Integration Impact Assessment) indicates that system and operational risks increase sharply after 30% renewable penetration, due to resource unavailability, grid instability, and resource inflexibility. Mr. Bakke discussed how portfolio evolution creates a reliability imperative for change and how MISO is working on transformational enhancements to ensure continued reliable operations.

Niki Schaefer, RF Vice President and General Counsel, provided an overview of the recently issued Executive Order on securing the U.S. Bulk Power System (BPS). She reviewed the Order's restrictions on the use of BPS equipment designed, developed, manufactured or supplied by a foreign adversary, which poses an undue risk to BPS security and safety. Ms. Schaefer also discussed next steps related to the Order and its implications for the ERO and stakeholders.

During the Compliance Committee meeting, Jeffrey Sweet, Director of Security Assessments at AEP, provided an overview of AEP's supply chain management program. He described AEP's multistep process, which includes a vendor risk determination, risk ranking, and security controls assessment. Mr. Sweet also shared ongoing enhancements to the program, including Asset2Vendor, which is an exchange for vendor assessment sharing among entities.



ReliabilityFirst Board of Directors and Committee Meetings will be held via WebEx August 12-13, 2020

Continuous Improvement - CI Foundations

By Sam Ciccone, Senior Reliability Consultant

The Journey to Security, Resiliency and Reliability

"A person and an organization must have goals, take actions to achieve those goals, gather evidence of achievement, study and reflect on the data and from that take actions again. Thus, they are in a continuous feedback spiral toward continuous improvement." - W. Edwards Deming

In the early 2000s, I was working for Schneider Electric in Lexington, KY. Since I worked for a disconnect switch manufacturer with products used in other manufacturing plants, we were able to tour another plant just a few miles down the road in Georgetown, KY. This plant was Toyota Motor Manufacturing Kentucky (TMMK).

Although our company was mostly mature in its processes, I had never seen anything like this well-oiled machine called TMMK. On that plant tour, I noticed production lines that provided space to work safely and efficiently and people (i.e., supervisors, line workers, and senior management) talking to each other. They were not just talking about the weather; they were collaborating and learning from each other to produce the highest quality automobiles.

Toyota had not only cemented itself as one of the top automobile manufacturers in the world, but it had become a role model for Continuous Improvement (CI). To read more about Toyota's CI Culture, a book I believe is a must-read is "The Toyota Engagement Equation"[1] written by former employees in the early U.S. plant days.

To build on Lew Folkerth's recent Lighthouse articles on the foundations of CIP Compliance, this article will provide some origins of CI, plus its foundations and principles. It will also delve into the foundations of the ReliabilityFirst Maturity Model assessment used to drive CI.

CI Origins, Principles and Methodologies

Continuous Improvement is a buzzword phrase, and most companies have practiced some variation of it since the 1800s. W. Edwards Deming, Walter A. Shewhart[2], and the founders of the Toyoda Automatic Loom Works Company (Sakichi Toyoda) and the Toyota Motor Company (Kiichiro Toyoda) are some of the founding fathers of CI.

Shewhart developed the Do-Check-Act (PDCA) cycle while working for the Western Electric Company. When Deming met Shewhart, he adopted and championed his methods. Deming later believed that PDCA was not sufficient and evolved it into Plan-Do-Study-Act (PDSA) in the 1990s. He argued that it is not enough to "check" that it happened to specs, but that it is important to "study" and learn from the outcome to share lessons learned throughout the organization. Both PDCA and PDSA are known as the "Deming Wheel."

Kiichiro Toyoda took many of the practices his father, Sakichi Toyoda, developed in his Loom factory and went on to hire Taiichi Ohnon who developed the Toyota Production Systems (TPS). This led to Kaoru Ishikawa combining the works of Ohnon and Shewhart/Deming into the TQM described below.

Here are a few methodologies that have evolved over the years. You may have heard or used a few of them under the umbrella of CI:

Kaizen – This is the Japanese word for CI. It is not a coincidence this philosophy originated in Japan where Toyota began. Principles include improve continuously, put an end to the "we've always done it this way" attitudes, and empower employees to solve problems. Kaizen is the Japanese term for "Change is Good" (Kai = Change, Zen = Good). Organizations use "Kaizen Events" to solve problems and improve processes by gathering folks from all aspects of the organization to work together toward CI.

TQM – Total Quality Management is a set of management practices utilized to consistently improve the end goal. As I shared from my observations at the Toyota plant, the core of TQM is

[1] The Toyota Engagement Equation: How to Understand and Implement Continuous Improvement Thinking in Any Organization

[2] Beyond The Phoenix Project: The Origins and Evolution Of DevOps (Official Transcript of The Audio Series)

Continued on page 4

Continuous Improvement - CI Foundations

Continued from page 3

the concept of CI — not just process improvements, but interaction among all levels of personnel and a basic CI culture and mindset.

Lean Manufacturing – Lean focuses on streamlining processes by eliminating waste in those processes.

Six Sigma – Developed in the 1980s, Six Sigma is a set of strategies, techniques and tools for process improvement that can be traced to an engineer who worked for Motorola. It means that through process improvement and consistency, you have achieved 3.4 defects in 1,000,000 opportunities.

DevOps[3] – DevOps, developed by Gene Kim, Kevin Behr and George Spafford, is a framework that stands on the shoulders of all these methodologies. It encourages Software Development Teams and IT Operations to work together to instill agility, reliability, resiliency and security within an organization.

RF Maturity Model

RF's Grid Reliability Improvement Maturity Model was developed using existing assessment models, such as CMMI (Capability Maturity Model Integration), CERT RMM (Resilience Management Model), and ES-C2M2 (Cybersecurity Capability Maturity Model). CMMI has been used by organizations such as NASA, Lockheed Martin, Microsoft and Motorola. RF adapted these models to develop the Maturity Model for the Electric Utility Industry.

This model contains Management Practices (groupings of internal controls) used to assess the maturity of the power grid. An assessment of these practices provides an organization with a snapshot of the current state of their processes in compliance, risk mitigation, and organizational maturity in Cyber Security, Operations, and Planning. It also provides a roadmap for improvement and is akin to performing the "plan" portion of PDSA.

Much like Lew explained in his recent Lighthouse articles on the foundations of CIP, these are the foundations of the RF Maturity roadmap to CI. The Assessments and the RF Maturity Model are located in the Internal Controls Knowledge Center on RF's website.

Many of the 16 management practices and their activities in the RF Maturity Model tie directly to Cyber and Physical Security. The following diagram provides a high-level view of some of these practices and relevant activities:

The CI theme presented here is PDSA, and Deming's quote in the beginning of this article alludes to the concept: "A person and an organization must have goals (**Plan**), take actions to achieve those goals (**Do**), gather evidence of achievement, study and reflect on the data (**Study**) and from that take actions again (**Act**)."

Utilities should strive for CI that will guide them on their road to Security, Resiliency and Reliability. I believe the first step (a.k.a. the first step in PDSA) is to assess where you are today because only then can you develop a plan to take the appropriate road to impactful improvement. For more information on how RF can guide you to CI excellence through the RF Assessment Process, please contact RF's Entity Engagement Department.

[3] The Phoenix Project: A Novel about IT, DevOps, and Helping Your Business Win

Get Control of Yourself - Things are Changing

By Denise Hunter, Principal Technical Auditor

The year 2020 appears to be all about change—pivotal changes and changes due to the "new normal." While the topic of updating an Entity Profile Questionnaire (EPQ) is not necessarily life changing, the intent is to help you identify your basic risk to the BPS and help focus any oversight activities on the appropriate areas.

The 2020 ERO Compliance Monitoring and Enforcement Program Implementation Plan (CMEP IP)[1] suggests that "registered entities should consider the risk elements and their associated areas of focus as they evaluate opportunities and their own prioritization to enhance internal controls and compliance operations focus."

The CMEP IP then identifies seven risk elements with applicable Standards and Requirements. Although, it's important to note that the CMEP IP also states, "For a given registered entity, requirements other than those in the CMEP IP may be more relevant to assist mitigating the risk, or the risk may not apply to the entity at all."

I believe one of the goals of the CMEP IP identification of ERO Risk Elements is two part:

1) to help entities identify their risk to the reliability and resiliency of the grid, and

2) to highlight the areas an entity should focus their efforts and funds toward establishing appropriate controls to mitigate those risks.

Toward that goal, RF is updating the EPQ with changes designed to help registered entities identify and communicate those ERO Risk Elements that apply to them, as well as any internal controls they might have in place to mitigate those risks.

ERO/RF Risk Elements
Management of Access and Access Controls
Insufficient Long-Term and Operations Planning Due to Inadequate Models
Loss of Major Transmission Equipment with Extended Lead Times
Inadequate Real-time Analysis During Tool and Data Outages
Improper Determination of Misoperations
Gaps in Program Execution
Texas RE: Resource Adequacy

What's Changing?

With the updated process, RF will ask if there have been any changes to key personnel or if any technology has changed. Key personnel refers to any personnel assigned to perform or monitor a key control[2].

Understanding changes to key personnel is important because those differences can impair an internal control. Incoming personnel initially may not be comfortable performing, or clearly understand the expectations of, the control. This could result in the control not performing as designed.

Depending on the risk the control is designed to mitigate, additional monitoring during this period may be warranted. Technology changes will always alter any existing controls, and the risk of human interaction with technology is often overlooked.

Controls such as reconciliations of data entry should be designed to remove the human risk.

Therefore, following the installation of any technology changes, a complete review of all controls related to the risk must be performed. The purpose behind these questions is to trigger an entity that has experienced one of these

[1] https://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/2020_ERO_CMEP_Implementation%20Plan.pdf

[2] A primary control that is essential for a consistent, appropriate process or to meet Standard expectations; typically takes place during the activity to which it applies

Continued on page 6

Get Control of Yourself - Things are Changing

Continued from page 5

activities to review their controls and ensure they are still adequate.

The updated EPQ also will include review of each ERO Risk Element, requiring registered entities to identify their risk score for each element. The score range is:

0 – No to Low Impact

2 – Low to Moderate Impact

4 – Moderate to High Impact

For example, if the registered entity is not required to provide modeling data, then their risk rating for the ERO Risk Element of Insufficient Long-Term and Operations Planning Due to Inadequate Models might be determined to be a zero. If the score is determined to be a zero, no further information is required.

If the determination is a two or a four, then additional questions will apply.

A few example questions:

- Are there documented internal controls related to that risk?
- And has monitoring of the internal control been defined?)

The registered entity will then have the opportunity to submit the documented control and evidence of monitoring.

Our goal with the changes to the EPQ was twofold. We added the new questions to assist entities in determining their risk to the BPS, thus establishing a baseline for needed internal controls.

This was coupled with the goal of maturing our understanding of our registered entities. The information submitted regarding your internal controls will help better define your Inherent Risk Assessment.

It also may assist in focusing any engagement and outreach activities to the appropriate risk area, thus improving reliability and increasing the efficiency of any oversight activities.

Change is challenging—and it often creates more questions than we may immediately have answers for, which can be frustrating. However, in order for the paradigm shift from compliance to risk to continue, change is inevitable.

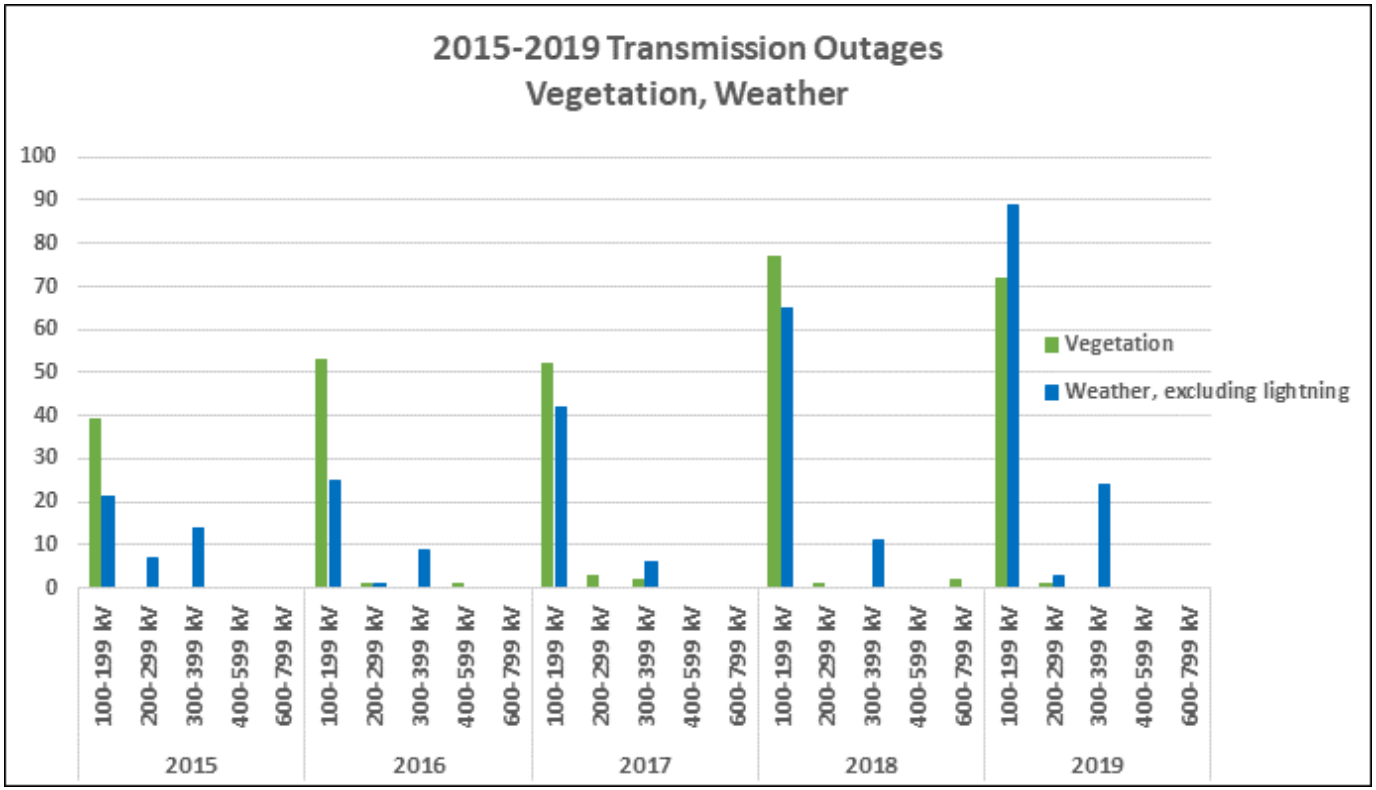
Be kind to each other and get control of yourself.

Join our Vegetation Management Group!

ReliabilityFirst has observed a steady upward trend in the vegetation-related outages on 100kV-199kV lines since 2015. Even though these outages are on lower voltage lines not applicable to FAC-003-4, they still pose a serious threat to the reliability of the BES as seen by historic events (e.g., Arizona-Southern California Outages).I

n an effort to mitigate this upward trend, RF has formed a Community of Practice (CoP) for Registered Entity vegetation management field personnel. A CoP is a group of people within a field of expertise that interact on a regular basis and seek to learn, share best practices, and collaboratively develop solutions to improve performance. This CoP is an informal gathering of vegetation management experts to review present issues, share lessons learned, and discuss success stories and/or near-misses in a confidential, technical environment. The goal is to build relationships across the RF footprint, reduce vegetation-related transmission outages, develop and improve safety practices, and gain work plan efficiencies to save cost. This CoP is meant to complement other groups, such as the North American Transmission Forum (NATF) and the SERC Vegetation Management Subcommittee, and target transmission-owning entities within the RF footprint.

Please note that this group is voluntary and available at no cost. Vegetation management professionals, if interested, should reach out to Thomas Teafatiller, Principal Engineer - Protection, to receive more information about this new initiative.



Summer 2020 Resource Adequacy Assessment

ReliabilityFirst performs a seasonal summer resource adequacy assessment based on data PJM and MISO provide. This article shares some highlights from MISO, PJM and RF assessments. For the summer of 2020, both MISO and PJM are expected to have an adequate amount of resources to satisfy their respective planning reserve requirements. The statistics included here support our analysis on outage risk, which concludes that there should not be an issue supplying demand within the RF Region this summer.

The COVID-19 pandemic is causing unique challenges for entities in both PJM and MISO footprints. The challenges focus around forecasting load and resources in the near term. The forecasted demand values identified in this report were calculated before the full effects of the pandemic were realized. PJM and MISO stated that current loads are below forecasted levels, but if the load does recover to the expected norms, resources should be adequate for this summer.

PJM Capacity and Reserves

Net Capacity Resources[1]	183,935 MW
Projected Peak Reserves	44,772 MW
Net Internal Demand (NID)	139,163 MW
Planning Reserve Margin	32.2%

The PJM forecast planning reserve margin of 32.2% is greater than the PJM margin requirement for the 2020 planning year of 15.5%. The margin for this summer is slightly higher than the 2019 forecast level of 31.9%. This is due to a decrease in NID when compared to last year.

MISO Capacity and Reserves

Net Capacity Resources	146,348 MW
Projected Peak Reserves	29,039 MW
Net Internal Demand (NID)	117,309 MW
Planning reserve margin	24.8%

The MISO forecast planning reserve margin of 24.8% is greater than the MISO margin requirement of 18.0% for the 2020 planning year. The margin for this summer is higher than the 2019 forecast level of 19.3%. This is mostly due to an increase in net capacity resources in MISO's market.

RF Footprint Resources

Net capacity Resources	201,548 MW
Projected Peak Reserves	41,103 MW
Net Internal Demand (NID)	160,445 MW
Total Internal Demand (TID)	171,786 MW

Since PJM and MISO are projected to have adequate resources to satisfy their respective forecasted reserve margin requirements, the RF region is projected to have sufficient resources for the 2020 summer period.

[1] Net capacity resources include existing certain generation and net scheduled interchange.

Continued on page 9

Summer 2020 Resource Adequacy Assessment

Continued from page 8

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. Reports and/or other data released by PJM, MISO or NERC for this same period may differ from the data reported in this assessment due to different assumptions that were made by RF from the onset of the report.

This analysis differs from NERC's in that RF uses actual historical Generator Availability Data System (GADS) data from a rolling five-year period, which provides a range of outages that occur during the summer period. The forecasted maintenance outages used in this analysis are derived from PJM and MISO for the summer months.

The stacked bar charts in Exhibits 1 and 2 are based on forecasted summer 2020 demand and capacity resource data for the PJM and MISO Regional Transmission Organizations (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 GADS outage data from May, June, July, August and September of 2015 through 2019.

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 (DR) are shown in shades of green. The firm demand constitutes the NID, with Total Internal Demand (TID) including the DR. The daily Operating Reserve requirement (shown in yellow) is between the NID and DR bars. The two sets of Demand bars represent the 50/50 demand forecast and the 90/10 demand forecast.

For instance, the 50/50 forecast projects a 50% likelihood that demand exceeds 139,163 MW. The 90/10 forecast is a more conservative model, projecting a 10% chance that demand exceeds 148,932 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.

While scheduled outages during the summer are generally minimal, there are planned scheduled outages reflected in the amount of Scheduled Maintenance (colored gray) in the Outage bar. The remainder of that bar represents the entire range of random outages (pink shows 100%; rose shows less than 100% down to 10%; and red shows less than 10% down to 0.1%) which occurred during the five-year reference period.

This analysis of random outages exceeding certain reserve margin targets is presented as a probability that is 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 listed reserve margin. They are discussed as probabilities as a matter of convenience in describing the analysis results.

To the left of the random outages range are probability percentages related to the amount of

Continued on page 10

Summer 2020 Resource Adequacy Assessment

Continued from page 9

outages that equal or exceed the amount shown above that line on the Outage bar.

Moving from top to bottom of the bar represents an increasing amount of outages, with a decreasing probability for the amount of outages. In the PJM chart, the random outages represented by the bar above the 100% point is 6,246 MW.

This means that the probability of there being at least 6,246 MW of random generation outages is 100%. Similarly, at the 10% point, the outages represented by the bar above the point is 19,274 MW (6,246 MW + 13,028 MW). There is a 10% probability that there will be at least 19,274 MW of outages. As shown by the probabilities and corresponding amounts, 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.

In Exhibit 1, the top of the 90/10 Demand obligation bar for PJM represents TID with operating reserves. The 1% line between the Outage bar and the 90/10 Demand bar represents the probability that there will be an amount of outages that will require Demand Response resources tobe utilized.This means that there is a probability of utilizing Demand Response during high demand (90/10).

Exhibit 2 contains the information to perform the same analysis for MISO. The top of the 90/10 demand obligation with the operating reserves has a 38% probability that DR will be required.

Exhibit 1 - 2020 Summer PJM Resource Availability Risk Chart

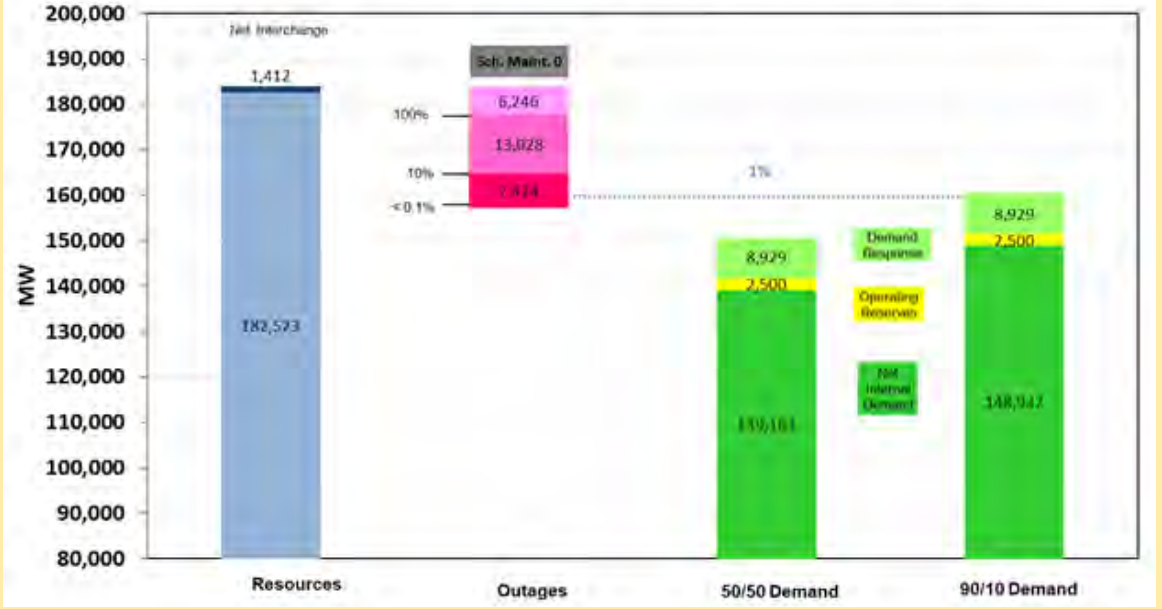
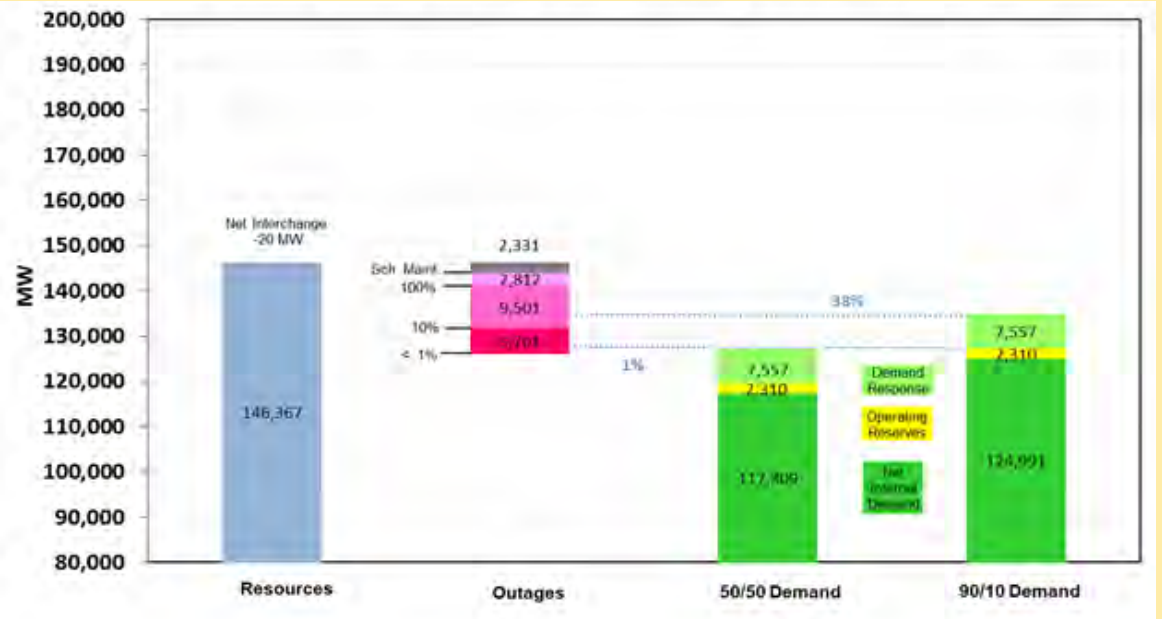


Exhibit 2 - 2020 Summer MISO Resource Availability Risk Chart



COVID-19 Impacts MISO Load Forecast

There is never a dull moment in load forecasting. Changes from the coronavirus (COVID-19) pandemic have presented new challenges.

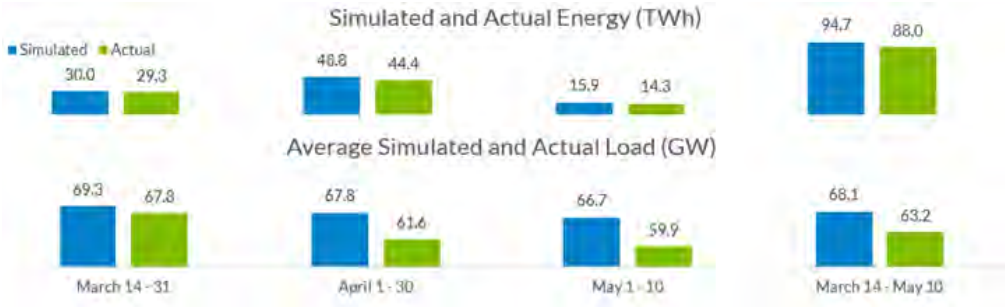
We continuously monitor and update our load forecast based on historic observations and weather forecasts to ensure reliability. Although changes in load have produced some interesting load patterns, causing us to adjust our load forecasts, they have not impacted reliable operations.

Has MISO observed any load behavior changes since mid-March?

Yes. MISO observed approximately 10% lower energy and demand than normal, as many residents stay at home. The timing and breadth of stay-at-home orders and closures of businesses vary widely across MISO's footprint.

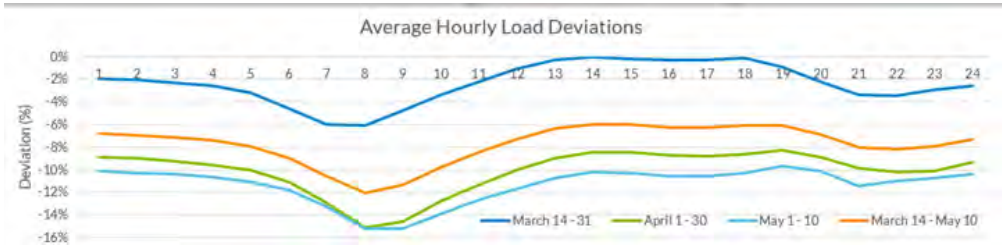
Therefore, the impact to load has been mixed. MISO's load levels declined slowly at first, and as more states issued stay-at-home orders, MISO saw additional load reduction. If and as these orders are lifted, MISO should start seeing higher load than recently observed.

COVID-19-related closures are progressively contributing to larger energy and load deviations (as shown by month)



MISO has observed that the morning peak hour is now occurring later. In addition, the evening peaks have been muted, as less electricity is used at night due to many retail and auto industry closures.

How does MISO determine the magnitude of the impact on load due to the COVID-19 pandemic?



Load impact is determined by running a backcast model using actual weather. This approach removes the weather bias, creating a reliable comparison to historical information.

Freezing the model prior to COVID-19 removes the load shape adjustments and model adaptation to recent history. The difference between the pre-COVID-19 model and actual load would be a "load deviation" from normal, as depicted in the graph.

Have there been any changes in the Load Forecast Model?

Yes, MISO attempted to reduce the load forecast errors. Initially, a manual override of the load forecast was implemented to lower the load forecast. Then, a new model variable was added on April 20.

Following that addition, the model has stabilized so that weather deviations are having more of an impact in May than changes due to widespread stay-at-home orders. Load forecast errors are not impacting reliable operations.

By Lew Folkerth, Principal Reliability Consultant

Foundations - Part 2

In this recurring column, I explore various questions and concerns related to the NERC Critical Infrastructure Protection (CIP) Standards. I share my views and opinions with you, which are not binding. Rather, this information is intended to provoke discussion within your entity.

It may also help you and your entity as you 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 also may 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.

This article continues the discussion of the background needed in order to be a proficient CIP professional. For the purposes of this article, I'll assume you're new to the CIP Standards, but this material should be useful to all CIP professionals, even if only as a review.

Understand the CMEP and the CMEP Processes

The Compliance Monitoring and Enforcement Program (CMEP) is Appendix 4C to the NERC Rules of Procedure. It describes how the Reliability Standards are monitored, assessed and enforced.

There are seven compliance monitoring processes defined in the CMEP. Think of these processes as seven general ways that Standards can be monitored for compliance.

1. Compliance Audit (audit) is probably the best known of the compliance monitoring functions. An audit consists of a formal review of compliance. The scope of an audit (or other CMEP process) consists of the Standards and Requirements under review, as well as the time period considered by the review. Audits may be conducted on-site (at the Registered Entity's site) or off-site (via teleconference). Audits are typically scheduled well in advance, but an unscheduled audit may be initiated with a notice of ten business days.

2. Self-Certifications are sometimes used when a new Standard comes into effect, or for other lower-risk issues. A Registered Entity is required to certify its compliance with a Standard. A self-certification should be treated as a self-audit with a specified scope. In most cases, entities are asked to supply the supporting documentation they used to arrive at their self-assessment.

Frankfort South and North Breakwater, MI – Photo: L Folkerth

3. Spot Check is very similar to a Compliance Audit but usually has a limited scope. Spot Checks are usually conducted off-site.

4. Compliance Investigations are in-depth reviews of a very specific compliance area and can be triggered by a system disturbance, a Complaint, or other indication of non-compliance.

5. Self-Report is a submittal by a Registered Entity that reports a possible instance of non-compliance to CMEP staff. As no compliance program is perfect, Self-Reports are an expected occurrence by entities with robust compliance programs and strong internal controls. Self-Reports are encouraged by mitigating credit being permitted in penalty calculations. Some Registered Entities are granted approval to perform **Self-Logging** for minimal-risk issues instead of submitting a full Self-Report.

6. Periodic Data Submittals are used for some Standards that need frequent but routine monitoring. For

Continued on page 13

Continued from page 12

example, FAC-003-4 is monitored in part by quarterly Data Submittals of vegetation outage reports.

7. Complaint is a report by a third party to NERC or a Regional Entity of possible non-compliance on the part of a Registered Entity. A Complaint may be submitted anonymously.

In my opinion, any CIP professional should be very familiar with the CMEP processes outlined here. I suggest you read and study Appendix 4C.

Understand Compliance Tools

The Reliability Standard Auditor Worksheet (**RSAW**) is the document used to communicate your approach to compliance with a Standard.

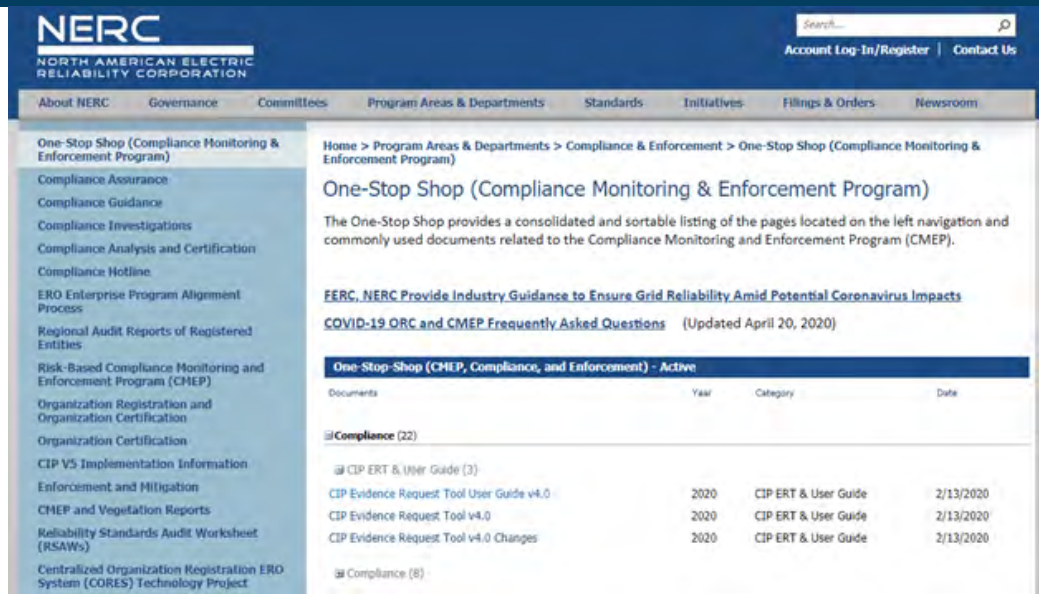
For a CMEP monitoring engagement (audit or spot check) within the RF footprint, you obtain the RSAW for a Standard from the NERC website and fill it out prior to the monitoring engagement. You will supply, in the appropriate sections:a list of subject matter experts responsible for the Standard, a list of evidence being supplied to demonstrate compliance with each Requirement or Part, and a narrative of how you achieve and maintain compliance with the Requirement or Part.

CMEP staff will typically follow the flow in the Compliance Assessment Approach section when evaluating evidence of compliance. This section of the RSAW also can give you valuable insight into how a monitoring engagement will proceed.

The narrative section of the RSAW is the most important part of the submission. It's your chance to convey to the audit team, in your own words, what the Standard means to you and how you approach compliance with the Requirement or Part. My article in the May 2015 RF Newsletter (available here) provides an in-depth look at the CIP RSAWs.

The CIP Evidence Request Tool (**ERT**) complements the RSAW by providing a common structure and format for submitting compliance evidence. You can see at any time what types of evidence will be requested for a monitoring engagement and what form the evidence should take during submission.

The ERT consists of the CIP Evidence Request Tool User Guide and the Evidence Request Tool spreadsheet. The current version of these documents can be obtained on the NERC website by hovering over “Program Areas & Departments” on the top menu and selecting “Compliance & Enforcement” from the pop-up menu. Then select “One-Stop Shop (Compliance Monitoring &



Enforcement Program)” from the left menu. Open the “Compliance” section and then open the “CIP ERT & User Guide” section.

Requests for Assistance

If you are an entity registered within the RF Region 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 RF website here.

Back issues of The Lighthouse, expanded articles and supporting documents are available in the RF CIP Knowledge Center.

Feedback

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

Lew Folkerth, Principal Reliability Consultant, I maybe reached here.

Executive Order on Securing the United States Bulk Power System

On May 1, President Trump issued an Executive Order on Securing the United States Bulk-Power System (Order). The Order discusses how the unrestricted foreign supply of bulk power system (BPS) equipment allows foreign adversaries to create and exploit vulnerabilities in BPS equipment, with potentially catastrophic effects. The Order outlines additional required steps to protect the security, integrity, and reliability of the BPS, summarized below. Additional details can be found on the Department of Energy resource page.

A. Prohibitions, Mitigating Measures, and Pre-Qualified Equipment and Vendors

The Order prohibits the "acquisition, importation, transfer, or installation" of BPS equipment where the Secretary of Energy (consulting with other departments and agencies)[1] has determined that the transaction: 1) involves BPS equipment designed, developed, manufactured, or supplied subject to the control, jurisdiction or direction of a foreign adversary; and 2) poses an undue risk of sabotage to the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of the BPS, or otherwise poses an unacceptable risk to national security and safety.

The Secretary may approve mitigating measures to allow a transaction to take place that would otherwise be prohibited by the Order. The Secretary also may establish and publish criteria for recognizing specific equipment and vendors as pre-qualified for future transactions and may apply the criteria to establish and publish a list of pre-qualified equipment and vendors. (However, the Secretary may still prohibit or otherwise regulate any transaction involving pre-qualified equipment or vendors).

B. Next Steps

Within 150 days of the date of the Order, the Secretary will publish rules or regulations implementing the Order. Additionally, as soon as practicable, the Secretary will:

(i)identify BPS equipment designed, developed, manufactured, or supplied, by individuals owned, controlled by, or subject to the jurisdiction or direction of a foreign adversary that poses an undue risk of sabotage or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of the BPS, poses an undue risk of catastrophic effects on the security or resiliency of critical infrastructure or the economy, or otherwise poses an unacceptable risk to national security, and

(ii)develop recommendations on ways to identify, isolate, monitor, or replace such items as soon as practicable, taking into consideration overall risk to the BPS.

C. Task Force on Federal Energy Infrastructure Procurement Policies Related to National Security

The Order establishes a Task Force on Federal Energy Infrastructure Procurement Policies Related to National Security (Task Force), which will coordinate federal procurement of energy infrastructure, as well as the sharing of risk information and risk management practices to inform this procurement.

The Task Force will be chaired by the Secretary and will include the Secretary of Defense; Secretary of the Interior; Secretary of Commerce; Secretary of Homeland Security; Director of National Intelligence; Director of the Office of Management and Budget; and the head of any other agency the Chair designates. Because attacks on the BPS can originate through the distribution system, the Task Force will engage with distribution system industry groups.

The Task Force will:

1. Develop a recommended consistent set of energy infrastructure procurement policies and procedures for agencies;

2. Evaluate the methods and criteria used to incorporate national security considerations into energy security and cybersecurity policymaking;

3. Consult with the Electricity Subsector Coordinating Council and the Oil and Natural Gas Subsector Coordinating Council in developing the recommendations and evaluation described in items 1 and 2 above;

4. Conduct other studies and develop other recommendations as directed by the Secretary; and

5. Submit annual reports to the President summarizing its progress, findings, and recommendations.

[1]Note that in most instances where the Order directs the Secretary of Energy to take an action, the Order states that the Secretary shall do so in consultation with other departments and agencies.

Standards Update

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

General NERC Standards News

NERC Implements Temporary Expanded Self-Logging Program Related to COVID-19 Impacts

On May 28, 2020, NERC implemented a new approach to COVID-19 linked noncompliances by expansion to its Self-Logging Program. NERC released an overall guidance document outlining the new regulatory approach. Additionally, NERC provided a template form to be used in the submittal process. Highlights of the program include the following:

- All entities are eligible for this temporary expansion of Self-Logging, and previous admission to the Self-Logging program is not necessary.
- Both minimal and moderate risk noncompliances relating to COVID-19 impact can be submitted as a part of Expanded Self-Logging.
- Under this temporary expansion of the Self-Logging Program, potential noncompliance related to coronavirus impacts and logged consistently with this guidance is expected to be resolved without further action.

Other COVID-19 Relevant Resources Posted

NERC/FERC have posted the following additional resources:

- In order to provide additional guidance regarding standards and compliance application resulting from COVID-19 NERC and FERC created a FAQ Spreadsheet about Joint NERC–FERC Industry Guidance for COVID-19.

Notable NERC Filings

In May-June, NERC filed the following with FERC:

- NERC submitted a petition for approval of proposed Reliability Standard CIP-002-6.
- NERC and WECC submitted a response to FERC's data request regarding proposed regional Reliability Standard BAL-002-WECC-3 (Contingency Reserve).
- NERC submitted a notice of withdrawal by NERC of its petition for approval of proposed Reliability Standard VAR-001-6.

Standards Update

New Standards Projects

New Standards projects are described on the NERC Standards website, along with links to all drafts, voting results, and similar materials. Recent activity includes:

Project	Action	Start/End Date
Comment Period Open for Proposed Changes to NERC Rules of Procedure:	Comment Period	5/21/2020 - 7/10/2020
New Standards Projects		
Regional Reliability Comment Period: PRC-006-5 WECC Variance **Project 2019-04 - Modifications to PRC-005-6**	Comment Period Comment Period	5/21/2020 - 7/6/2020 6/2/2020 - 7/8/2020
Recent and Upcoming Standards Enforcement Dates **(Please see notes in "Notable NERC Filings" section regarding the deferment of some of the following standards.)**		
April 1, 2020	CIP-003-8 – Cyber Security – Security Management Controls	
October 1, 2020	CIP-005-6 – Cyber Security – Electronic Security Perimeter(s); CIP-010-3 – Cyber Security – Configuration Change Management and Vulnerability Assessments; CIP-013-1 – Cyber Security – Supply Chain Risk Management	
January 1, 2021	PRC-002-2 – Disturbance Monitoring and Reporting Requirements (50% compliance for Requirements 2-4, 6-11); PRC-025-2 – Generator Relay Loadability, phased-in implementation of Attachment 1: Relay Settings, Table 1 Options 5b, 14b, 15b, and 16b by six months (January 1, 2021); CIP-008-6 – Cyber Security – Incident Reporting and Response Planning; PRC-012-2 – Remedial Action Schemes	
April 1, 2021	PER-006-1 – Specific Training for Personnel; PRC-027-1 – Coordination of Protection Systems for Performance during Faults	
July 1, 2021	TPL-007-3 – Transmission System Planned Performance for Geomagnetic Disturbance Events (Requirements 11 and 12)	
January 1, 2022	TPL-007-3 - Transmission System Planned Performance for Geomagnetic Disturbance Events (Requirements 6, 6.1-6.4, 10, 10.1-10.4)	
July 1, 2022	PRC-002-2 – Disturbance Monitoring and Reporting Requirements (100% compliance for Requirements 2-4, 6-11)	
January 1, 2023	TPL-007-3 – Transmission System Planned Performance for Geomagnetic Disturbance Events (Requirements R3, R4, 4.1. 4.1.1–4.1.2, 4.2, 4.3, 4.3.1, R8, 8.1, 8.1.1–8.1.2, 8.3, 8.4, and 8.4.1)	
January 1, 2024	TPL-007-3 – Transmission System Planned Performance for Geomagnetic Disturbance Events (Requirements R7, 7.1, 7.2, 7.3, 7.3.1–7.3.2, 7.4, 7.4.1–7.4.3, 7.5, and 7.5.1.)	

These effective dates can be found here.

Enhancing the Reliability and Compliance Open Forum Call

ReliabilityFirst's regularly scheduled Open Forum Call is an important opportunity to share pertinent information and hear from our stakeholders, so we are excited to announce that we are enhancing the call to better serve our Region. The call will still take place at 2:00 p.m. EST every third Monday of the month, and we will continue to offer the same helpful compliance-related content and Electric Reliability Organization (ERO) updates.

What's New?

To build upon the typical information shared during these calls, we are expanding into other risk areas and engaging subject matter experts throughout the BES to tackle risks such as cyber security, misoperations, and situational awareness. The RF team is working hard to provide content that not only helps entities prepare for upcoming audits and spot-checks, but also dives into the risks facing the RF footprint.

We also are making these additional changes:

- Starting in **July (the call is on Mon. 7/20)**, the call will have a new name, as well as a new WebEx link and password for each call. The link and details will be available in the Upcoming Events section of the RF website.
- We will be using Slido (a virtual Q&A/polling tool) to solicit responses to help tailor our content, gather additional feedback on your questions and concerns, etc.
- The calls will be extended from 60 minutes to 90. While we may not use the entire 90 minutes for every call, the extension will allow for additional time to interact with our entities.

Who Should Dial In?

In an effort to ensure the information provided reaches audiences beyond our Primary Compliance Contacts (PCC), we are now posting the agendas to our website further in advance and including them in our monthly compliance letter. This will give PCCs enough time to invite their colleagues who would benefit from joining the call. **Please invite your Operations, Planning, Cyber, Design, IT, and/or Maintenance personnel, if you see an agenda topic they would be interested in!**

What if I have Other Questions?

Although these calls are not the venue for entity-specific questions, the RF Assist Visit program is available all year – with the added bonus of a quicker response than waiting until the next call. Our program is customized to fit your needs, whether it be help with an individual compliance requirement, assistance regarding a risk area (e.g., misoperations), or a maturity evaluation.

We are always happy to work with our entities before or after an audit to stay engaged, learn from industry peers, and share our knowledge. Please feel free to fill out the Assist Visit form on our website so that we can put you in touch with the right SMEs to help you out.

If we receive questions or concerns about the same topic from multiple entities, we can address those topics during these Open Calls to share with the larger group. We look forward to hearing from you!

Upcoming Open Forum Calls

The tentative agenda of topics to be covered by RF staff during the July 20 call includes:

Misoperation Information Data Analysis System (MIDAS)

- This is especially relevant for Transmission Owners and Generator Owners responsible for submitting misoperation information. Please invite protection system SMEs and those responsible for compiling and submitting this data to RF.

PRC-024 Generator Frequency and Voltage Protective Relay Settings

- This is especially relevant for Generator Owners and others responsible for testing and programming relay settings to ensure generating units remain connected during defined frequency and voltage excursions.

Operational Resilience

- This is especially relevant for SMEs in the areas of cyber, IT/OT and physical security, as well as any personnel involved in operations or securing the BPS. Please invite anyone in your organization interested in learning about assessing and benchmarking your cyber resilience.

Agendas will be available closer to the dates of the remaining 2020 calls:

August 17	October 19
September 21	November 16

SAVE THE DATE

2020 Fall Workshop Webinar

Tuesday, August 25

New Compliance Oversight Plan FAQ

In response to the questions received during the May 18, 2020 Reliability and Compliance Open Forum Call, a Compliance Oversight Plan (COP) FAQ document was created to aid in entities' understanding of the enhanced COP Report.

For any additional questions regarding the FAQ or COP Report in general, please visit our Contact Us page and direct your question to the Risk Analysis & Mitigation group.

Workshops will now be held via WebEx - Register Today

Webex login information will be emailed out to registrants closer to the event date.

Protection System Workshop for Technical Personnel • August 18, 2020

Register

ReliabilityFirst is hosting its sixth annual protection system educational workshop for technical personnel via Webex.

This Protection System Workshop for Technical Personnel will cover a diverse range of topics and discussions relative to Protection Systems tailored to the needs of technical personnel and will include speakers from RF, industry subject matter experts, and others. Topics slated for discussion include capacitor bank protection, protection simplicity, and IEC 61850 regarding communication in substations.

Intended Audience

- Substation Electricians/Supervisors
- Substation Field/Commissioning Engineers Relay Technicians
- Relay Engineers and others who work directly with this equipment
- Communications Engineers/Technicians
- Company Trainers on this subject
- Others interested in these topics

2020 Human Performance Improvement (HPI) Overview • August 19, 2020

Register

New for 2020, there will be a half-day session on the morning of August 19 for a Human Performance Improvement (HPI) Overview by Dr. Jake Mazulewicz.

This overview session is intended for those that are new to the human performance arena or who just want to refresh their knowledge of human performance principles and concepts.

Human Performance Workshop for Technical Personnel • August 20, 2020

Register

ReliabilityFirst will be hosting our annual human performance workshop this year via Webex.

This workshop will focus on practical application of human performance techniques and concepts for front-line activities that attendees can retain and use in transmission reliability related work areas such as operations, asset management, design, protection, maintenance, and others.

Intended Audience

- Substation and Transmission maintenance
- Protection and Controls
- Operations Control Rooms, including tools support personnel for EMS, SCADA, etc.
- Asset Design groups (substation and transmission)
- Asset Management groups
- Other leaders interested in these topics

RF Staff Excels at Professional Development

ReliabilityFirst prides itself on being an indispensable industry resource, and the steady stream of certifications and accolades obtained by our staff illustrates that the value RF offers entities and stakeholders goes well beyond enforcing the delegated functions of the CMEP. We encourage you to take advantage of the impressive breadth and depth of expertise exhibited by staff.

The following list is a snapshot of the achievements earned by the RF team over the past year, so please join us in congratulating them on their accomplishments!

Patrick O'Connor, Counsel – Patrick obtained an ANSI-accredited Certified Information Privacy Professional Certification through the International Association of Privacy Professionals. This elite certification is the world's first broad-based global privacy and data protection credentialing program, and it focuses on the legal requirements for the responsible transfer of sensitive data.

Lew Folkerth, Principal Reliability Consultant, Entity Engagement – Lew obtained a GIAC Penetration Tester Certification (GPEN) through the SANS Institute. GPEN certification holders have the knowledge and skills to conduct exploits and engage in detailed reconnaissance, as well as utilize a process-oriented approach to penetration testing projects.

David Sopata, Principal Reliability Consultant, Entity Engagement – David obtained a GIAC Response and Industrial Defense (GRID) Certification from the SANS Institute. The certification focuses on Active Defense and Incident Response toa ddress industrial control system cyber attacks to maintain the safety and reliability of operations.

Beth Rettig, Technical Auditor, O&P – Beth obtained her MBA from Syracuse University with a specialization in Business Analytics and Supply Chain Management.

Zack Brinkman, Manager, CIP – Zack is now a Certified Information Systems Security Professional (CISSP) after obtaining this certification from the International Information System Security Certification Consortium.

Kristie Purcell, Configuration Management Specialist – Kristie obtained a Business Analysis Program Certificate from Baldwin Wallace University.

Nate Hill, Desktop Analyst – Nate is now a Certified Windows Security Administrator (GCWN), which is his second GIAC Certification. This certification focuses on the configuration and management of the security of Microsoft operating systems and applications.

Calendar of Events

The complete calendar of RF Upcoming Events is located on our website here.

Date	RF Upcoming Events	Location
July 20	Reliability and Compliance Open Forum Call	Conference Call
August 12	ReliabilityFirst Board of Director Committee Meetings	WebEx
August 13	ReliabilityFirst Board of Director Meeting	WebEx
August 17	Reliability and Compliance Open Forum Call	Conference Call
August 18	6th Annual Protection System Workshop for Technical Personnel	WebEx
August 19	Human Performance Improvement (HPI) Overview	WebEx
August 20	3rd Annual Human Performance Workshop	WebEx

Industry Events:

Date	Industry Upcoming Events
June 23-25	FERC - Technical Conference regarding Increasing Market and Planning Efficiency and Enhancing Resilience through Improved Software, Washington, DC
June 25	FERC - Technical Conference regarding reliability of the Bulk-Power System, Washington, DC)
September 1-2	NERC - GADS Wind Training
September 23-24	NERC - Monitoring and Situational Awareness Technical Conference, Golden, CO
September 29- October 1	NERC - Electric Power Human Performance Improvement Symposium, Denver, CO
October 20-23	NERC - GridSecCon (no location noted)

ReliabilityFirst Members

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

Forward Together RF ReliabilityFirst

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