PUBLIC

RELIABILITY FIRST

Issue 2 | 2023 Q2

Cultivating a Talented & Engaged Workforce

ReliabilityFirst Corporation
3 Summit Park Drive, Ste 600
Cleveland, OH 44131
(216) 503-0600
www.rfirst.org

Note from the President

Dear Stakeholders,

The summer ahead is an important one. This August will mark the 20th anniversary of the 2003 Northeast Blackout that saw approximately 50 million people in the U.S. and Canada lose power.

There will no doubt be media coverage of this historic date in the months ahead as well as heightened attention on our industry. Obviously, a lot has changed since then, but it's a sober reminder of why it's important to follow the standards we now have in place and strive to improve on them as we work to stay ahead of the new challenges on the horizon.

In our industry we do a tremendous job of learning from events, like the blackout of 2003. We learned a lot from that experience and made many corrections to the electric system. But it's my hope that we can continue to be more forward-looking, especially as we put newer and newer technologies into the grid, and that we can anticipate things happening and stop them from happening before a risk is realized.

Our projections for this summer show that in the RF region, both PJM and MISO are expected to have adequate resources to satisfy their planning reserve requirements under 50/50 demand forecasts. While this is good news, we must remain prepared to face more extreme scenarios should they occur.

In this issue, you'll read all about the theme of "people." The "why" of ReliabilityFirst (RF) always comes back to the people who depend on our industry to provide their electricity. When something like a blackout occurs, it reinforces how important electricity is. And at the end of the day, it's also people who do the necessary work to keep the lights on each and every day and prevent bad days like the blackout of August 2003 from occurring.

At RF, our people are at the core of what we do, and we've prioritized our workforce in our Strategic Plan, which we'll outline in this issue. We'll also dive into ways your organization can work toward building a strong workforce through recruitment, retention, training and diversity, equity and inclusion initiatives in Continuous Improvement.

This summer, let us take a moment to appreciate the importance of striving to keep improving in our quest to stay ahead of the many challenges we face to keeping the electric grid reliable and secure, and also the power of people to make a difference.

Forward Together,

Tim

Issue 2 | 2023 Q2

INSIDE THIS ISSUE

Follow us on:

Strategic Plan: Cultivate a Talented and Engaged Workforce

A letter from Vice President Diane Holder

Dear Stakeholders,

At the start of the year, we unveiled to you our 2023-2027 Strategic Plan. My colleague Jeff Craigo introduced the plan and its first strategic objective, to be an excellent regulator, in the first quarter newsletter.

Our second strategic objective is one that resonates deeply with me personally: to cultivate a talented and engaged workforce. I see every day the impact our talented staff makes in the work we do, and as part of RF's leadership team, overseeing our Human Resources department, I know this is something that cannot be taken for granted.

For me, the remarkable work we do is a direct result of the collaborative efforts and contributions of our amazing team members. That's why it was vital to us as an organization to call this out in our Strategic Plan – we see it as fundamental to our ability to perform our necessary function of keeping the electric grid reliable and secure.

To achieve this objective, we aim to maintain these guiding principles:

1. Recruit, retain and train the right people for the right roles;
2. Further enhance and promote diversity, equity and inclusion;
3. Prioritize our positive workplace culture.

In 2022, we increased our retention rate by 8% from 2021, up to 93%. I am also proud to say we are making progress on our diversity, equity, and inclusion initiatives. Since 2019, we've made a 5% increase in the diversity of our workforce, increased the number of our female employees by 10% and increased our female leadership by 100%. We hope to continue to grow these figures in the years to come. And I am humbled to share that in June, RF was recognized by Cleveland.com and the Plain Dealer as one of the top workplaces in Northeast Ohio. This is the fourth year in a row we've received this distinction and I am grateful to all our staff that make RF such an enjoyable place to work through their consistent demonstration of teamwork, respect, and commitment to excellence.

Going forward, RF faces the same workforce challenges many companies do, from the great resignation, changing demographics and the lasting effects of the COVID-19 pandemic – but we will continue to do all we can to prioritize our people and our culture as we work to continue to serve the public good in maintaining a secure and reliable electric grid.

Forward Together,

Diane Holder, Vice President, Entity Engagement & Corporate Services

Continuous Improvement

By Sam Ciccone, Principal Reliability Consultant, Entity Engagement

Cultivating a talented and engaged workforce

The Journey to Security, Resiliency and Reliability

"You don't build a business - you build people - and then people build the business."
— Zig Ziglar, author and motivational speaker

People are arguably the most important aspect of a successful organization. RF's Strategic Plan includes the recruitment, retention and training of people, the promotion of diversity, equity, and inclusion (DEI), and the prioritization of a positive workplace. Not only are these specific and separate goals, but for successful organizations that value their people first, they are also interconnected.

Recruiting the right people lays the foundation for achieving the other goals in this strategic objective. For many companies though, this line of thinking is not at the forefront. About 40% of U.S. companies outsource much, if not all, of the hiring process, according to research by organizational consulting firm Korn Ferry. And only about a third of U.S. companies reported that they monitor whether their hiring practices lead to bringing good employees on board, according to a 2019 Harvard Business Review article.

So, what are some best practices for recruitment? One is that recruitment is more than finding candidates that check off the boxes in a job description. You should also hire for the potential these candidates bring. This will supply a larger pool of resources to choose from.

Retention, which ties directly to recruiting, makes you ask the questions: why are people leaving, and what makes them stay? Retention is problematic due to a myriad of reasons including salary, being overworked, absence of work life balance, and poor workplace culture. These are all things that we as a regulator and you as an electric utility need to work on, especially understanding that this leads to a highly secure, resilient, and reliable power grid. If you can't retain the right people, it leaves gaps in knowledge that can trickle down to the proper operation of our power grid.

For more information, see SERC Reliability Corporation's article titled "Will there be enough skilled workers in the future?"

Recruiting and employment agency Robert Half suggests ways to improve retention of valued employees. One tactic is ensuring salary and other compensation are at least on par with the market value for similar positions. When people feel like they are underpaid, they look elsewhere. Ensuring proper compensation far outweighs the cost of replacing those employees.

Another strategy is to attempt to post jobs internally, not just externally. This develops trust and sends the message to existing employees that they can advance in their current organization. Fostering an environment where employees feel they can speak their minds is another potential pathway to improving retention.

This includes companies not just meeting with employees twice a year during performance reviews, but also providing periodic feedback on performance and managers offering help when employees face an issue or are struggling with an aspect of their role.

Once you bring in the people, training, education, and awareness are vital. In our industry, training and awareness should extend not only

Continued on page 5

Continuous Improvement

Continued from page 4

The ERO encourages a systematic approach to training. As an example, NERC Standard PER-005-2 states that "Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall use a systematic approach to develop and implement a training program for its System Operators".

to employees, but also to contractors, vendors, and consultants. Awareness brings about desired behaviors in support of a bulk electric system that is secure, resilient, and reliable and that supports a risk-aware culture. Training remediates the skill gaps of new and existing staff, and if the skill gaps pose risks to the organization, they should be properly addressed by some form of risk management developed by the organization. Lastly, education goes beyond training, making sure employees can better respond to unique circumstances, which is crucial for the security, resilience, and reliability of the grid.

Diversity, equity, and inclusion (DEI) is also tied to recruitment, as well as culture (discussed next). Per our Strategic Plan, "*We champion diversity by acknowledging, respecting, and including all races, genders, ages, ethnicities, orientations, religious backgrounds, and identities. We ensure equity by examining our procedures and processes so that everyone is treated fairly regarding pay, access, and opportunities.*"

Some of the key benefits of DEI initiatives are that they foster innovation and help to avoid group think. DEI is also essential to building a workplace where people want to work. More than 70% of job-seekers are looking to work for a company with a dedicated commitment to DEI, according to research from the University of Pennsylvania Wharton School of Business. And companies are 35% more likely to experience greater financial returns if they have a diverse workforce, according to research from consulting firm McKinsey & Company.

Lastly, our Strategic Plan emphasizes the prioritization of a positive workplace culture. At RF, we strive to foster a culture that encourages employees to engage and bring their authentic selves to work each day, that recognizes and incentivizes well-being and innovation, and that provides platforms to encourage team building, wellness, learning more about ourselves and our teammates, and recognizing and empowering each other. We are not alone in prioritizing a strong company culture – 94% of executives believe it's key to business success, according to research from Deloitte.

Continuously improving your recruitment, retention, training, DEI program, and culture is not easy. All of these are complex moving targets that affect each other. But organizations that make it a priority to improve in these areas have happier employees that want to stay, create a more diverse pool of employees that bring value from their different perspectives, background, and education, and show an increase in a positive workplace culture.

As the quote from Zig Ziglar at the beginning of this article alludes to, people are the starting point that can propel the growth and sustainability of a successful organization. These are things that we should all strive for, not only for compliance and reliability, but to stay on top of an ever-changing grid and world we live in today.

Summer Resource Assessment

By Tim Fryfogle, Principal Engineer - Resources, Engineering & Systems Planning

RF performs a seasonal summer resource adequacy assessment based on data provided by PJM and MISO.[1] This article shares some highlights from the MISO, PJM, and RF assessments. For the upcoming summer of 2023, under projected 50/50 demand forecasts, both MISO and PJM are expected to have adequate resources to satisfy their respective planning reserve requirements.

However, if resource outages and/or demand are experienced beyond the established projections, there is an increased likelihood that both Load Modifying Resources and Operating Reserves would need to be utilized to serve forecasted load.

The risk assessment, outlined below, evaluates the capability of both MISO and PJM to meet their planning reserve requirements under random resource outage scenarios based on historic Generator Availability Data System (GADS) outage data. While this analysis concluded that there should not be an issue of having enough resources to supply demand within the RF Region for the 2023 summer, there is an elevated risk if resource unavailability and load demand are higher than anticipated.

Within MISO, there is a risk of not meeting periods of higher than anticipated peak demand if wind generator energy output is lower than expected. Furthermore, the need for assistance from external (non-firm) resources during more extreme demand levels will also depend largely on wind energy resources and their output, if available.

PJM Capacity and Reserves

As listed in the table, the anticipated PJM forecast planning reserve margin of 31.9% is greater than the required PJM planning reserve margin for the 2023 planning year of 14.9%. The planning reserve margin for this summer is slightly higher than the 2022 forecast level of 31.7%.

MISO Capacity and Reserves

The MISO forecast planning reserve margin of 23%, seen in the table above, is greater than the required MISO planning reserve margin requirement of 15.9% for the 2023 planning year. The planning reserve margin for this summer is higher than the 2022 forecast level of 21.1%. This is mostly due to a decrease in Net Internal Demand (NID) and a larger amount of firm imports into the MISO region.

RF Footprint Resources

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 2023 summer period as seen in the table above.

PJM Capacity and Reserves	
Net Capacity Resources[2]	187,003 MW
Projected Peak Reserves	44,232 MW
Net Internal Demand (NID)	141,771 MW
Planning Reserve Margin	31.9%

MISO Capacity and Reserves	
Net Capacity Resources	143,668 MW
Projected Peak Reserves	26,843 MW
Net Internal Demand (NID)	116,825 MW
Planning Reserve Margin	23%

RF Footprint Resources	
Net Capacity Resources	222,659 MW
Projected Peak Reserves	62,258 MW
Net Internal Demand (NID)	161,401 MW
Total Internal Demand (TID)	170,696 MW

[1] The MISO results were developed on data submitted prior to their capacity auction published results on May 17, 2023, and presented to the public on May 19, 2023. Revised values from the capacity auction are not anticipated to significantly change the results or identified risk in this assessment.

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

Continued on page 7

Summer Resource Assessment

Continued from page 6

Random Generator Outage Risk Analysis

The following analysis evaluates the risk associated with random generator outages that may reduce the available resources below the load obligations projected for 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. This is due to different assumptions that were made by RF from the onset of the analysis. This analysis differs from NERC's in that RF used historical GADS data from a rolling 5-year period, which provided a range of outages that occur during the summer period (i.e., May through September). In contrast, the NERC Analysis polls each assessment area (i.e., MISO and PJM) and requests the average forced outages for weekdays in June through September, over the past three years. Both analyses provide a valid way to consider outage scenarios when projecting capacity and reserves. The forecasted maintenance outages used below are derived from PJM and MISO for the summer months.

The stacked bar charts in Exhibits 1 and 2 are the result of the RF analysis and based on forecasted Summer 2023 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 historic GADS outage data from May, June, July, August, and September of 2018 through 2022.[3]

Referring to Exhibits 1 and 2, the committed resources in PJM and MISO are represented by the Resource bar in shades of blue and only include the net interchange that is a capacity commitment to each market (i.e., firm transactions). Additional interchange transactions that may be available at the time of the peak are not included as they are not firm commitments and are therefore not allowed in the calculation to satisfy 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 Net Internal Demand, with Total Internal Demand including the Demand Response (DR). The daily Operating Reserve requirement

[3]The distribution of random outages used for this assessment is not linear throughout the range of outages observed.

Exhibit 1 - 2023 Summer PJM Resource Availability Risk Chart

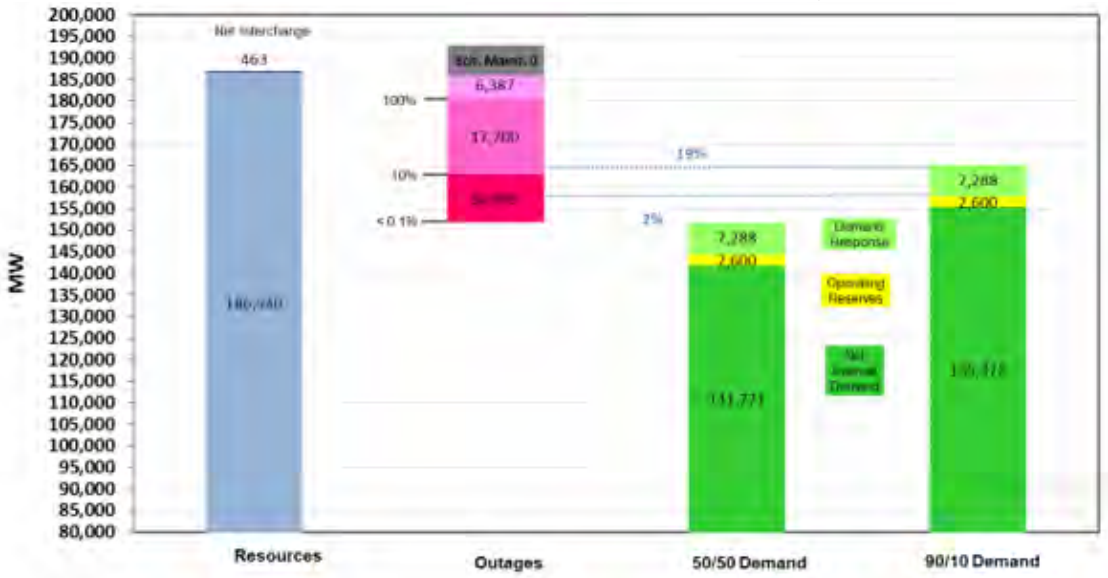
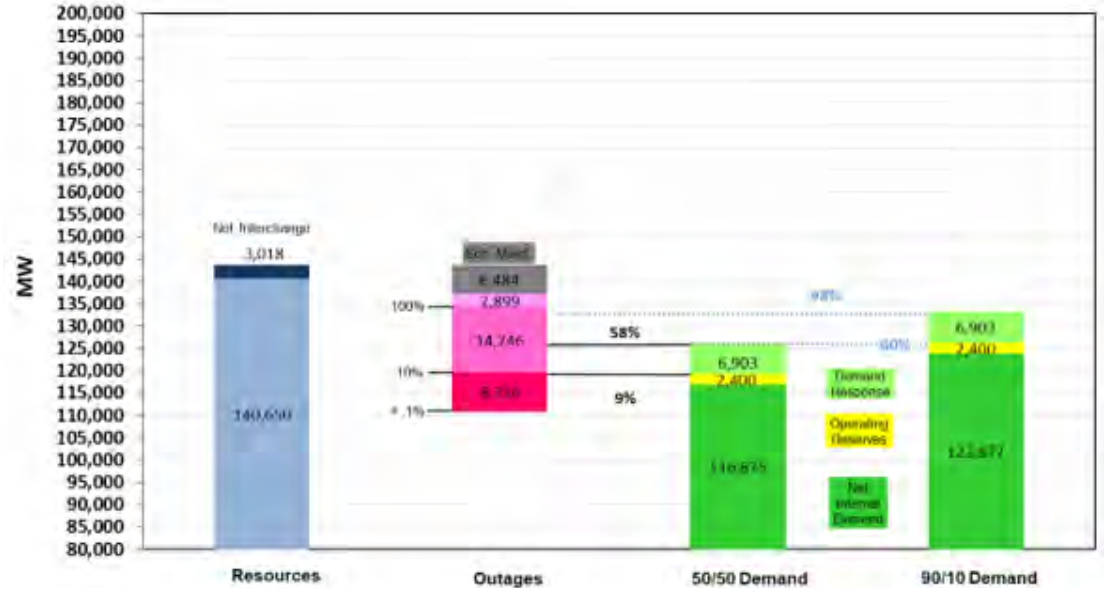


Exhibit 2 - 2023 Summer MISO Resource Availability Risk Chart



Continued on page 8

Summer Resource Assessment

Continued from page 7

(shown in yellow) is between the NID and DR bars. There are two sets of stacked demand bars on the chart, one representing the 50/50 demand forecast and one representing the 90/10 demand forecast. The 50/50 demand forecast projects a 50% likelihood that demand exceeds 141,771 MW. The 90/10 demand forecast is a more extreme model, projecting a 10% chance that demand exceeds 155,378 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.

Between the resources bar and the demand bars is the outages 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 Maintenance (colored gray) in the Outage bar. The remainder of the Outage bar represents the probability or entire range of random outages. The pink area shows 100% of the random outages; rose shows less than 100% down to 10% probability of the random outages; and red shows less than 10% down to 0.1 % of the random outages occurring as indicated on the chart. These probabilities occurred during the five-year reference period (i.e., 2018 to 2022).

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. They are discussed as probabilities as a matter of convenience in describing the analysis results.

It should be noted that the Planning Reserve Requirement for each study area is below the total resource outages identified by RF. As an example, PJM's is 14.9% which equates to 21,100 MW, while the largest 5-year rolling resource outages identified in GADS is 35,036 MW.

In Exhibit 1, the top of the 90/10 Demand obligation bar for PJM represents Total Internal Demand with operating reserves. The 19% line between the Outage bar and the 90/10 Demand bar represents the probability that resource outages could cause Demand Response resources to be utilized. The 2% line indicates that after all of the demand response is utilized and a high outage scenario is present, operators will have to use other mitigating steps to balance load and capacity. This means that once resource outages exceed 22,000 MW there is the potential for PJM to use DR and Operating Reserves to meet their internal load during a high demand (90/10) scenario.

Exhibit 2 contains similar information to perform the same analysis for MISO. The top of the 50/50 Demand obligation with Demand Response and Operating reserves is 58%. During normal operating conditions, there is a 58% probability that resource outages could require Demand Response resources to be utilized. This means that once the random outages and schedule maintenance exceed 11,000 MW the potential for utilization of DR and Operating Reserves increase during the 50/50 scenario. The top of the 90/10 demand obligation with the operating reserves has a 98% probability that Demand Response will be required during high demand. Once the random outages and schedule maintenance exceed 10,500 MW, the potential for utilization of DR and Operating Reserves increases during the 90/10 scenario.

In the PJM chart (Exhibit 1), the random outages represented by the bar above the 100% point is 6,387 MW. This means that the probability of there being at least 6,387 MW of random generation outages is 100%. Similarly, in the MISO Chart (Exhibit 2) at the 10% point, the outages represented by the bar above the 10% point is 17,645 MW (2,899 MW + 14,746 MW). This indicates that there is a 10% probability that there will be at least 17,645 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 outages bar are the probabilities of the random generation outages that correspond to different levels of demand obligation. In other words, and referring to Exhibit 2, this means there is a 98% probability that Demand Response could be needed to meet the 90/10 demand scenario.

Through stakeholder engagements, RF is encouraging all Generator Owners to carefully coordinate fuel supply, availability, and planned/unplanned outages with their Reliability Coordinators throughout the summer to address these risks.

The Lighthouse

By Lew Folkerth, Principal Reliability Consultant, External Affairs

Preparing for Internal Network Security Monitoring (INSM)

What is INSM?

Internal Network Security Monitoring, or INSM, is the practice of understanding what is going on inside your networks. For the purposes of the CIP Standards, that means understanding what network traffic is occurring within your Electronic Security Perimeters (ESPs).

Today's CIP Standards only require monitoring of traffic into and out of an ESP. INSM is different in that it is monitoring of traffic within an ESP or other network.

Why is INSM important?

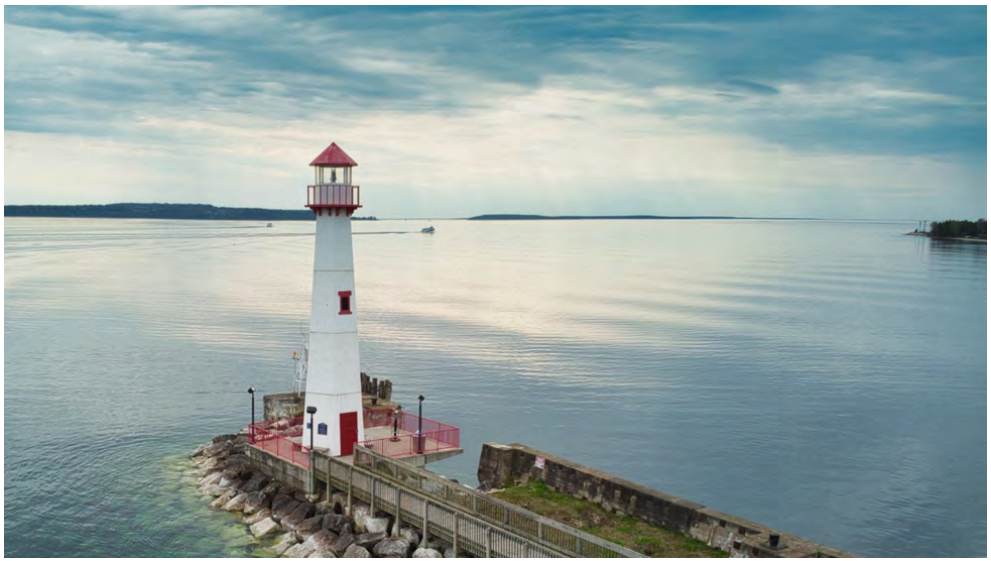
INSM addresses the risk of a malicious actor bypassing your ESP firewall and gaining network access to your ESP. Some malicious actors can evade detection by signature-based defenses such as antivirus solutions or intrusion detection systems.

In that case, there may be no way to detect that presence in your network without INSM. To address this risk, FERC issued Order 887.

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.

Order 887

On January 19, 2023, FERC issued Order 887, *Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems*. FERC directed NERC to "develop new or modified CIP



Wawatam Light, St. Ignace, Michigan – Photo: Lew Folkerth

Reliability Standards requiring INSM for all high impact BES Cyber Systems with and without external routable connectivity and medium impact BES Cyber Systems with external routable connectivity to ensure the detection of anomalous network activity indicative of an attack in progress." [Order 887 at P3]

NERC is required to ensure revisions to the CIP Standards achieve the following security objectives [paraphrased from Order 887 at P79-80]:

1. Develop a baseline for network traffic by analyzing network traffic and data flows for security purposes.
2. Monitor for and detect unauthorized activity, connections, devices, network communication protocols, and software inside the CIP-networked environment, as well as encompass

Continued on page 10

Continued from page 9

awareness of protocols used in industrial control systems.

3. Methods to ensure:
   a. logging of network traffic,
   b. maintaining those logs, and other data collected, regarding network traffic that are of sufficient data fidelity to draw meaningful conclusions and support incident investigation, and
   c. maintaining the integrity of those logs and other data by implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures.

Note that INSM is an industry security practice, while Order 887 calls for implementing INSM via revised CIP Standards.

What is the timeline for Order 887?

NERC is required to file the INSM revisions in mid-2024, so it's reasonable to expect an Effective Date for any new or revised Standards to be sometime in 2027. This estimated date will be influenced by many factors, so please don't hold me to this.

What preparation will be needed for INSM?

INSM is not a project where you can just buy some gear, install it, and be done. INSM will require getting extremely familiar with your Cyber Assets, the software they run, the protocols they use to communicate with other assets, and how the communications data flows under different conditions. Here are some things to consider when beginning your INSM journey:

Staffing – Entities large enough to have high or medium impact BES Cyber Systems will almost certainly need additional staff to implement INSM. Your staff will need to understand your operational environment, so just re-assigning IT staff may not be sufficient.

Also see the article, "Cultivating a Talented and Engaged Workforce," in this Newsletter.

Training – Operational environments have specialized needs and require specialized skillsets. You will probably need to provide training for your operational security personnel, beyond that of typical IT training. Such training could be provided by vendors, by independent training organizations, or by your own specialists. The specialized skills needed will include understanding of the protocols being used within your networks and how those protocols are used by your equipment and processes.

Initial monitoring points – You will need visibility into your applicable networks in order to begin developing your baselines. This will require carefully selecting one or more points in your network to begin monitoring. These initial points could be in a test or development network rather than in a production network.

Initial baseline – You will need to understand all the protocols in use and what those protocols are used for. Start small and begin working to build your network understanding and visibility.

Baseline minimization – You may want to consider ways to reduce the amount and types of traffic on your ESP networks. If possible, replace systems that generate unnecessary traffic with systems whose traffic you can tightly control.

Network segmentation – You may want to consider employing VLANs within your applicable networks to create multiple network segments with less traffic per segment. This can make your monitoring tasks easier by focusing on a smaller set of traffic per VLAN segment. Also, unauthorized traffic may stand out better if there is less traffic on the segment.

Continued on page 11

Continued from page 10

Monitoring strategy – As you gain a deeper understanding of your internal networks, you can develop or improve your monitoring strategy. Will you use network switch span ports? Will you use ethernet taps to create a shadow network for monitoring? Other techniques? Or a combination of techniques? Consider looking at other types of security programs within your entity, such as insider threat management.

Storage planning – You will need to store your monitoring data such as the retained logs or traffic captures. This data has the potential to be very large, so begin planning for that storage now. Since we don't yet know how long this data will be required to be stored, assume a substantial period of time such as a year. Due to the potentially large size of the data to be stored, you may want to consider a separate storage system for INSM data.

Information protection – After the information is gathered and stored, its confidentiality, integrity and availability will need to be protected. Include these plans in your overall strategy.

When should my entity start preparing for INSM and Order 887?

INSM is a detective control you can implement on any network, although it is especially valuable on sensitive networks such as ESPs. As such, it is a good idea to begin implementing INSM as a "best practice" security control without waiting for the revised standards to become effective.

While I expect the Effective Date for the Standards resulting from Order 887 could be in 2027, I strongly encourage you to begin your preparations now. You should identify your staffing and training needs and start addressing those needs. Don't wait until FERC approves the new requirements. Take advantage of the lead time being offered by the FERC Order and begin developing your staff, your baselines, and your monitoring strategies now.

References

- Order 887
- CMEP Practice Guide – Network Monitoring Sensors
- Project 2023-03 INSM Standard Development Page

Participate!

You have many ways you can participate in the standards development effort. You can volunteer for the drafting team. You can attend drafting team meetings. You can assist your entity in writing comments on the revised standards. You can influence your entity's vote on the revised standards. You can do any or all of these, but please get involved!

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, can be reached here.

Continued on page 10

Internal Controls

By Courtney Fasca, Technical Auditor, Operations & Planning

People play an important role in growing the maturity of your internal controls program

"I never pick up an item without thinking of how I might improve it. I never perfected an invention that I did not think about in terms of the service it might give others."

-Thomas Edison

Internal controls are essential to any sustainable program you aim to build within your organization, and at their foundation are people. In the mindset of Thomas Edison, picking up a control and evaluating it is your opportunity to make it better and provide a service to all who use the control. It's on people to not only implement and follow internal controls, but to examine them and think about ways they can be made stronger.

To assess the maturity of the programmatic or global internal controls program at an entity, we at RF lean on the framework offered by the GAO Green Book. It lists five components that make up a strong internal controls program, and people are present throughout each of these components:

1. Control environment
2. Risk assessment
3. Control activities
4. Information and communication
5. Monitoring of each of the above components

When talking about the control environment, we are assessing an entity's commitment to integrity and ethical values, the established structure and responsibility with enforced accountability, and the commitment to competence. Is the drive for continuous improvement echoed throughout the company, from the top all the way down? Are staff held accountable for performing controls, and is risk-targeted training being provided? Are staff positively recognized for identifying gaps and mitigating risk in an effort for continuous program improvement?

Rather than implementing internal controls in a reactive nature (such as in response to audit findings), is the entity proactively measuring and leveraging information to identify these areas of improvement? And when the entity identifies these opportunities, are they documented so they can be passed along? You may recall last year's Q2 article, "Do You Have Documented Internal Controls?", where we discussed on-the-job "fixes" and staff tribal knowledge that double as (often undocumented) internal controls.

In our evaluations of an internal controls program, we observe each entity's risk assessment. Is a periodic risk assessment – with clear, defined objectives – being performed? Does this assessment of risk include external interdependencies and quantify risk? Does it go beyond just compliance risk?

Of course, we also dive into control activities. We do this on a control-by-control basis as well, but when looking at the overall internal controls program, we have more broad questions: are the controls just in one business unit, or do they exist across the company? Are there layers of controls with measurable results that can be communicated and built upon? Are staff empowered and encouraged to improve upon processes?

Continued on page 13

Internal Controls

Continued from page 12

We assess the entity's information and communication strengths – again, is communication more reactive or is it proactive and periodic in nature? Is it limited to just within business units, or is data made available to appropriate personnel for opportunities to improve processes and controls? Perhaps data is aggregated across multiple business units, and the entity leverages that relevant information in helpful metrics and dashboards? Is the entity communicating not only internally, but externally? Is the entity interacting and measuring themselves with their peers, looking for best practices? Is information being collected to track potential deficiencies?

And finally, we assess the entity's monitoring activities. As mentioned previously and in the 2023 Internal Controls Workshop, relying on RF performing spot checks or audits should not be your sole monitoring activity. While it is important to ensure the entity is improving in response to CMEP activity results and in response to events, it is equally important for the entity to conduct periodic evaluations of their internal controls and internal controls program – ensuring controls are designed efficiently and are performed as expected.

When RF evaluates your internal controls program, we aren't looking to give you a violation or a PNC based on your program. A lack of established internal controls by itself does not indicate potential non-compliance. We know that internal controls are a critical component of risk-based auditing – the assurance of *continued* compliance. Your ability to demonstrate how your internal controls program makes your organization better – with the focus on always continuously improving – is what we at RF are truly looking for and want to celebrate success around.

A sustainable program built on strong internal controls starts with you. Focus on the people component of your internal controls program – people are important to establishing an active continuous improvement culture. From top executives to the individual contributors and subject matter experts, everyone in your organization has a part to play.

If you are looking for more guidance or have an area or risk you'd like to focus on for an appraisal, please feel free to reach out to RF's Entity Engagement group.

Visit the Contact Us page on our website and select Entity Engagement from the drop-down menu to get in touch.

Enforcement Explained

By: Mike Hattery, Counsel, Enforcement

A Concerning Trend in VAR-002-4.1 R1 and R3

In Enforcement, beyond focusing on individual cases, we spend time zooming out on open and closed actions to assess whether we are seeing any broader trends across standards or registration functions. With that in mind, this column is focused on an uptick in VAR-002-4.1 issues among Generator Operators (GOPs).

VAR-002-4.1 is in the operations and planning space, and underlying compliance activities involve the performance of high-frequency conduct, especially VAR-002-4.1 R2 (maintaining voltage with a specified schedule). It is "high-frequency" in that it is a continual operational requirement, and the continual nature (or number of associated acts) elevates the probability of noncompliance occurring. Although it does not excuse noncompliance, this is a relevant consideration.

Enforcement's concern relates to VAR-002-4.1 R1 (GOP operating interconnected generator in automatic voltage control mode) and R3 (GOP shall notify its associated TOP of a status change on the automatic voltage regulator, power system stabilizer,[1] alternative voltage controlling device within 30 minutes of the change).

The Size and Nature of the Uptick

Since the start of 2020, RF has taken in 32 VAR-002-4.1 R1 or R3 noncompliances. Obviously, pure volume of noncompliances alone is not an indicator of heightened risk. However, we are seeing a high concentration of certain root causes or common failure types among a single registration type, which warrants further evaluation and discussion.

Additionally, VAR-002-4.1 R1 and R3 are fundamental building blocks for system stability. When units are not in automatic voltage control mode, operator interaction is necessary, and during a system event, the system operator may not know or react fast enough to provide the proper reactive support needed to maintain system voltage. Without proper reactive support, the Bulk Power System (BPS) could experience voltage depression, voltage exceedance, or loss of load due to reactive resources not responding as needed or required.

Common Failure Types

When it comes to disarming automatic voltage control mode or the operation of Power System Stabilizers (PSS), the root causes and incidents of failure are remarkably similar. They are best understood in two buckets:

1. the initial act of an entity disabling or failing to enable automatic voltage control mode or PSS; and
2. an entity's persistent failure to identify that it did not enable automatic voltage control mode or PSS.

We often see these common failure types occur when a generating asset is taken offline and then brought back online. Specifically, we've seen this when generators are taken out of operation for maintenance, operation verification, or for more material repairs. We less frequently see the failure occur when the asset is de-energized; rather, we see the failure most frequently when generators are re-energized.

[1]Hereinafter, "PSS."

Continued on page 15

Enforcement Explained

Continued from page 14

Generally, this is the result of haphazard generator restarts where either: (a) the entity's energizing process lacks adequate detail on how to confirm automatic voltage control mode or PSS status during a start-up; or (b) the execution of start-up is rushed, and the relevant procedure is ignored.

Beyond how the condition is most frequently initiated, we are also seeing automatic voltage control mode or PSS continue in a disabled state for sustained periods of time without proper notification because the entity does not have adequate alarming controls, or those alarming controls are not properly configured. We are seeing entities without audible alarms or pop-up alarms on their SCADA system for where PSS or automatic voltage control mode are not enabled, which can cause the condition to continue until a voltage issue arises if the items are missed at start-up. In fact, in multiple instances, entities identified that automatic voltage control mode was disabled while they were experiencing issues achieving their voltage schedule.

What to do?

1. Entities should review site procedures for start-up/energizing steps and evaluate the quality of the procedural steps and the likelihood they will drive enabling PSS, automatic voltage control mode, or AVR where appropriate.
    a. Consider adding multiple checkpoints or prompts in the process for enabling PSS or automatic voltage control mode and then confirming functionality.

2. Entities should review their identifying and alarming controls for automatic voltage control mode, and PSS operability. If the entity or a specific site does not have an alarm or notification likely to drive action when the tools are errantly disabled, consider implementing such an alarm.

3. Entities should review their applicable voltage schedules and compare their voltage alarm setpoints to ensure that deviations will be identified, as alarming controls are also relevant for VAR-002-4.1 R2.
    a. Consider implementing a periodic comparison of the applicable voltage schedule and alarm setpoints.

Enforcement Approach

At RF, VAR-002-4.1 R1 and R3 incidents are of increasing concern and represent "low-hanging fruit" in the effort to improve the probability of success in the struggle of maintaining voltage stability on the BPS. These items are simply too easy to get right or identify quickly (as well as too important as useful tools for voltage stability) for lapses to continue with such frequency and duration.

Contact Entity Engagement

We encourage registered entities to reach out to our Entity Engagement team if they have questions regarding their approach to VAR-002-4.1.

High Tide

By Tony Freeman, Principal Analyst, Risk Analysis & Mitigation

A Guide to Emerging Risks

Volume 1: How Bulk Electric System Cyber Security Information (BCSI) is compromised and how your organization can safeguard its information

Welcome to the first installment of High Tide. Each quarter we will be selecting an emerging risk, explaining what RF is seeing, providing a general awareness, and discussing some potential controls to consider in mitigating those risks.

In the recent past, there have been issues relating to protecting BCSI. Most of these issues have stemmed from three origins: accessibility, mishandling and mislabeling of BCSI. BCSI often includes the asset name, locations, or actionable process steps that may be leveraged if an incident were to occur. Without the proper protections in place, the BCSI documents could potentially provide a nefarious actor with a playbook on how to circumvent your controls and procedures, which could highlight points of weakness in your security programs.

The following items describe the three main origins of what RF has seen recently:

Accessibility

Data accessibility concerns often stem from these three areas:

1. BCSI is accessible by unauthorized personnel through:
    a. Improper provisioning of access due to unclear processes/procedures.
    b. Lack of procedural adherence.
2. Vendors or contractors mishandle BCSI due to:
    a. Contract language not containing verbiage to adequately describe how BCSI should be handled/ stored.
    b. Training is inadequate and not fully understood by contractor/vendor personnel.
    c. Training does not provide appropriate level of detail for vendor/contractor to fully understand entity’s systems and procedures.
3. Access is not revoked in a timely manner for individuals who no longer need it, which creates the potential for unauthorized transfer of data from the system(s), due to:
    a. Vendors/contractors not providing notification that individuals have resigned or been terminated in the required timeframes.
    b. Revocation of access for employees or vendors/contractors is not completed within the required time frame due to lack of procedural adherence.
    c. Revocation processes/procedures are misunderstood or ambiguous and contributors are unaware of the appropriate steps to complete the revocation action.

Mishandling

Data is often mishandled in one of the following ways:

Data is removed or copied from BCSI storage containers in violation of security policies/procedures and distributed, recreated, or otherwise mishandled/manipulated. This can occur through the following ways:

1. BCSI is printed or replicated and not stored in an approved storage container.
2. Vendors/contractors do not follow proper contract language and transfer/copy BCSI to their PCs locally and security controls cannot be verified.
3. BCSI is dispersed beyond entity control.

Mislabeling

Data mislabeling occurs quite often when BCSI labels are overlooked or misassigned. This can happen during creation or during annual reviews, when BCSI isn't recognized, causing it to be mislabeled, stored outside of a BCSI storage container and without access restrictions.

Continued on page 17

Continued from page 16

Controls to consider to mitigate or reduce potential risks

With the right controls in place, it is possible to safeguard BCSI and protected data. Here are some controls your organization should consider:

1. Develop processes, procedures, training, and awareness campaigns to protect BCSI.
    a. Make sure access roles are discussed to ensure proper provisioning for different types of BCSI such as by department, by role, or other indicators.
    b. Develop checklists and desktop procedures to make processes/procedures quick and easy to understand for all involved.
    c. Ensure that training is applicable to all individuals who could potentially need or be provisioned access to BCSI.
    d. Provide security training to staff and contractors/vendors that includes topics discussing BCSI identification, storage, and handling.
2. Review documentation periodically to ensure proper labeling and storage.
    a. Prevent human error by having a peer review or multi-person reviews of documentation.
3. Routinely review access to BCSI/protected data, identifying what documentation applies to what teams/departments and ensuring no improper access has been granted or retained.
    a. One option is to use a segmented approach, such as grouping by departments, job, function, leadership role, etc.
    b. Another option is to establish “data owners” who are responsible for the upkeep and overall protection of subsets of BCSI that are applicable to their work area.
4. Review vendor’s/contractor’s documentation:
    a. Establish Contractual Terms and Conditions for BCSI, data handling, and storage with vendors and contractors. Utilize a “trust but verify” approach ensuring that those terms and conditions are being followed by vendors and contractors.
    b. Ensure vendors/contractors are properly trained in accordance with your data policies and procedures.
5. Limit exposure by reducing access to files, ensuring that files are not electronically transmitted and that vendors/contractors are conducting documentation reviews on premises under entity supervision.
6. Ensure BCSI storage containers and locations are properly identified and protected. Ensure documentation naming conventions/labeling leave no room for error in BCSI identification.
    a. Ensure labels are visible on all required documentation in places such as headers, footers, or even large watermarks.
7. Ensure policies and procedures cover physical copies of BCSI, including when it is permitted to be printed, from what locations, when duplication is authorized, and how it is stored, handled in transit, and ultimately destroyed if appropriate.
    a. If needed, designate areas in which physical copies of BCSI can be viewed.
    b. In instances of physical copies, it may be wise to retain logs of when copies are removed from physical locations, by whom, when they are returned, or if they are destroyed.

By taking a proactive approach you can prevent the misuse of BCSI, ensuring a better security posture. This prevents the circumvention of all the hard work, hours, and resources that go into building controls to protect and secure systems. Remember that the protection and handling of BCSI is not limited to an annual review but should be reviewed often to maintain the integrity of the BCSI program and the systems to which BCSI is referencing.

If you have any questions, comments or concerns regarding risk analysis, mitigation, or evidence please feel free to contact Tony Freeman at Tony.Freeman@RFirst.org, RF Risk Analysis and Mitigation (RAM) department.

NERC Issues Report on Effectiveness of CIP-014 Physical Security Standard

On April 20, NERC issued a report in response to FERC's order directing NERC to study the effectiveness of the current CIP-014 physical security standard. In the order, FERC directed NERC to address three questions:

- Are the applicability criteria of CIP-014 adequate?
- Is the risk assessment adequate, considering information gathered during compliance audits of the standard?
- Should a minimum level of physical protection be established for all BPS transmission stations and substations and primary control centers?

NERC's report, Evaluation of the Physical Security Reliability Standard and Physical Security Attacks to the Bulk-Power System, states that the CIP-014 applicability criteria makes the standard applicable to the overwhelming majority of the 345kv and all 500kv substations, and there is no evidence that expanding it would identify additional substations as critical. Therefore, NERC does not recommend expansion at this time but will work with FERC staff to hold a technical conference on whether additional substations should be studied for potential inclusion in the applicability criteria.

NERC's report also finds that there should be more detailed requirements for performing the CIP-014 risk assessment (used to identify which substations should be deemed "critical" under the standard). NERC evaluated compliance and enforcement data and found that entities had inconsistent approaches to performing the risk assessment. Additional specificity in the CIP-014 language should help address this issue, and NERC will initiate a new standard development project to work on these additions.

Finally, NERC does not recommend a "common minimum level of physical security protection" for all BPS transmission stations, substations, and primary control centers at this time, as more study is needed. However, NERC acknowledges the need to further evaluate resiliency and security measures to mitigate risks associated with physical security attacks and wishes to work with FERC on a technical conference to gather additional data on protection, response, and resiliency measures and discuss whether they should be incorporated into reliability standards or guidelines.

Fiscal Responsibility Act of 2023 requires NERC to Conduct Interregional Transfer Capability Study

President Biden has signed into law new debt ceiling legislation, titled the "Fiscal Responsibility Act of 2023." Along with raising the debt ceiling and limiting federal spending, the act contains provisions that are relevant to FERC, the ERO Enterprise, and the electric industry.

Notably, Section 322 of the act requires NERC, in consultation with the Regional Entities and entities that span multiple transmission planning regions, to conduct a study of total transfer capability between transmission planning regions. (The act defines total transfer capability as "the amount of electric power that can be moved or transferred reliably from one area to another…of the interconnected transmission systems by way of all transmission lines [or paths] between those areas under specified system conditions, or [as defined by] the Reliability Standards").

The study must include the following:

- Current total transfer capability between each pair of neighboring transmission planning regions.
- A recommendation of "prudent additions" to total transfer capability between each pair of neighboring transmission planning regions that would strengthen reliability.
- Recommendations on how to meet and maintain the total transfer capability (including the study's recommended additions to the total transfer capability) between each pair of neighboring transmission planning regions.

Within 18 months, NERC must submit the study to FERC, who will then publish the study and seek comments on it. Within one year of the public comment period, FERC must submit a report to Congress on its conclusions from the study and any recommendations for statutory changes resulting from the study.

FERC issues Orders to Bolster Reliability during Extreme Weather

On June 15, FERC issued two orders to bolster reliability during extreme weather events. In the first order, Transmission System Planning Performance Requirements for Extreme Weather, FERC directs NERC to submit modifications to Reliability Standard TPL-001-5.1 (or to create a new standard) within one year to require transmission system planning for extreme heat and cold weather conditions. Specifically, the standard must require:

1. The development of benchmark planning cases based on prior extreme heat and cold weather events and/or future meteorological projections.
2. Planning for extreme heat and cold weather events using steady state and transient stability analyses that cover a range of extreme weather scenarios, including the expected resource mix's availability during extreme weather conditions and the wide-area impacts of extreme weather.
3. Corrective action plans that include mitigation for any instances where performance requirements for extreme heat and cold events are not met.

In the second order, One-Time Informational Reports on Extreme Weather Vulnerability Assessments, FERC directs transmission providers to submit one-time reports describing their current or planned policies and processes for conducting "extreme weather vulnerability assessments" and identifying mitigation strategies. The order defines an extreme weather vulnerability assessment as an analysis that identifies where and under what conditions transmission assets and operations are at risk from the impacts of extreme weather events, how those risks will manifest themselves, and what the consequences will be for system operations.

Transmission providers are required to file one-time informational reports within 120 days on how they conduct extreme weather vulnerability assessments (if at all), including details on how they:

1. establish a scope;
2. develop inputs;
3. identify vulnerabilities and exposure to extreme weather hazards;
4. estimate the costs of impacts; and
5. use the results of vulnerability assessments to develop risk mitigation measures.

FERC issues Order 893 providing Incentive Based Rates for Cybersecurity Investments

On April 21, FERC issued a final rule, Order 893, providing incentive-based rates for utilities making certain voluntary cybersecurity investments that materially improve cybersecurity and are not already required by the CIP Standards or otherwise legally mandated. The order makes incentive-based rates available:

1. To utilities that make voluntary cybersecurity investments in Advanced Cybersecurity Technology (any technology, operational capability, or service, including computer hardware, software, or a related asset, that enhances security posture by improving the ability to protect against, detect, respond to, or recover from a cybersecurity threat), and/or
2. To utilities that participate in cybersecurity threat information sharing programs such as the Cybersecurity Risk Information Sharing Program (CRISP).

The order also creates the regulatory framework for utilities to request these incentive-based rates.

The order includes a list of pre-qualified investments (the "PQ List") that would satisfy the eligibility criteria.The initial items on the PQ List are:

1. investments associated with participation in CRISP, and
2. investments associated with internal network security monitoring that go beyond CIP Standard requirements.

FERC will periodically evaluate whether to add more items to the PQ List, and utilities can still seek FERC approval of investments that are not on the PQ List. Utilities can also seek FERC approval of investments related to voluntary early compliance with new CIP Standards before their effective dates.

FERC Order on Registration Work Plan for Inverter-Based Resources

On May 18, FERC issued an order approving NERC's three-year work plan on how NERC will identify and register owners and operators of inverter-based resources (IBRs) connected to the Bulk-Power System (BPS) that are not otherwise required to register under the bulk electric system (BES) definition.

In the order, FERC approves NERC's work plan and implementation timeline to:

1. revise its Rules of Procedure and Registry Criteria to include GO-IBRs as a new function (which NERC has clarified includes both owners and operators of IBRs),
2. identify candidates for GO-IBR registration within 24 months; and
3. register GO-IBRs within 36 months.

Additional technical details on who would fall under the GO-IBR function are contained within the order. NERC also states in its work plan that it plans to create a sub-set list of Reliability Standards that apply to GO-IBRs, and that it plans to evaluate whether changes to the BES Definition should be made in the future.

FERC Holds Forums on Gas-Electric Coordination and the PJM Capacity Market

On June 15, FERC held a forum on the state of the PJM capacity market. Panelists (including NERC CEO Jim Robb and PJM CEO Manu Asthana) discussed: 1) the purpose and outcomes of PJM's capacity market, 2) whether changes to it are needed considering the changing resource mix and resource adequacy concerns, and 3) potential capacity market design reforms. There was also a roundtable with state public utility commissioners on the capacity market. A recording of the forum is available here.

On June 20, FERC held a New England Winter Gas-Electric forum to discuss possible solutions to the electricity and natural gas challenges facing the New England region. Topics included studies on extreme weather risks in the region, the gas-electric infrastructure in the region, and infrastructure and market design reforms to help address electric and gas system challenges during New England winters. While the forum focuses on the New England region, much of the discussion on extreme weather and gas-electric coordination is relevant across the country. A recording of the forum is available here.

U.S. House of Representatives Subcommittee Holds Hearings on Reliability and Security

The U.S. House of Representatives Energy, Climate, and Grid Security Subcommittee (Subcommittee) held two hearings in June focused on reliability and security topics.

On June 13, the Subcommittee held a hearing titled "Oversight of FERC: Adhering to a Mission of Affordable and Reliable Energy for America." The FERC Commissioners were the witnesses at the hearing and discussed reliability concerns and FERC activities related to resource adequacy and the changing resource mix. The recording of the hearing is available here, as well as the Commissioner's testimonies: Chair Phillips, Commissioner Christie, Commissioner Danly, and Commissioner Clements.


Chairman
Willie L. Phillips


Commissioner
James Danly


Commissioner
Allison Clements


Commissioner
Mark C. Christie

On June 16, the Subcommittee held a field hearing in Moore County, North Carolina titled "Enhancing America's Grid Security and Resilience." During the hearing, the Subcommittee members discussed physical security and the recent substation attacks in Moore County.

The hearing witnesses included Mark Aysta (Managing Director, Enterprise Security, Duke Energy), William Ray (Director of Emergency Management, North Carolina Department of Public Safety), Tim Ponseti (Vice President, Operations, SERC), and Jordan Kern (Professor at North Carolina State University).

A recording of the hearing is available here, and witness testimonies can be found here: Mark Aysta, William Ray, Tim Ponseti, Jordan Kern.

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 Opens the 2023 Appendix 3D Registered Ballot Body Self-Select Attestation Process

Appendix 3D of the Rules of Procedure (ROP) provides for the establishment of the Registered Ballot Body and describes the process for selecting membership in the appropriate ballot body segment. Appendix 3D requires that each participant that self-selects a segment must then self-select annually. This action is completed via the Self-Select Attestation process. Each voting Registered Ballot Body member should log into the Standards Balloting and Commenting System and complete relevant activities by Aug. 15, 2023.

NERC Publishes TPL-001-5.1 Reliability Standard Audit Worksheet (RSAW)

NERC posted the RSAW for TPL-001-5.1 to the RSAW home page under the heading “Current RSAWs for Use.” The effective date of this standard is July 1, 2023. This standard implements certain system planning performance requirements.

Notable FERC Orders

In April-June 2023, FERC filed the following:

- On May 18, 2023, FERC issued an order approving NERC’s Registration Work Plan for inverter based resources.
- On April 14, 2023, FERC issued an order approving PRC-002-4. PRC-002-4 includes various disturbance monitoring and reporting requirements for Reliability Coordinators, Generator Owners, and Transmission Owners.

Notable NERC Filings

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

- On June 12, 2023, NERC and NPCC jointly filed comments for the 2023 New England Gas and Electric Forum. These comments address NERC and NPCC assessments performed relating to northeastern reliability.
- On May 15, 2023, NERC filed a petition with FERC for the approval of changes to Texas RE’s regional standards development process. The proposed revisions are summarized in the following manner in the petition: “[t]he changes include clarifying existing sections, revising processes to be more consistent with the NERC Standard Processes Manual, and increasing the flexibility for the Member Representatives Committee (or “MRC”) to make decisions regarding Texas RE Regional Standards development projects.”
- On April 20, 2023, NERC filed a report with FERC regarding CIP-014-3. The report was in response to a December 2022 FERC Order to review the efficacy of the Physical Security Reliability Standard in mitigating the risks to the Bulk-Power System (“BPS”) associated with physical attacks.

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. Please take note that some Enforcement Dates relate to specific requirements and sub-requirements of the Standard and are detailed below. Recent additions include the following:

Project	Action	Start/End Date
Project 2020-06 - Verifications of Models and Data for Generators	Initial Ballots and Non-Binding Polls	6/27/22 - 7/6/22
Project 2020-02 - Transmission - connected Dynamic Reactive	Comment Period	5/31/22 - 7/14/22

Recent and Upcoming Standards Enforcement Dates	
July 1, 2023	TPL-001-5.1 – Transmission System Planning Performance Requirements | Implementation Plan
Jan. 1, 2024	TPL-007-4 – Transmission System Planned Performance for Geomagnetic Disturbance Events (Requirements R7, 7.1-7.3, 7.3.1-7.3.2, 7.4, 7.4.1-7.4.3, 7.5, 7.5.1, R11, 11.1-11.3, 11.3.1-11.3.2, 11.4, 11.4.1-11.4.3, 11.5, and 11.5.1); CIP-004-7 – Cyber Security - Personnel & Training; CIP-011-3 – Cyber Security – Information Protection
April 1, 2024	FAC-003-5 – Transmission Vegetation Management; FAC-011-4 – System Operating Limits Methodology for the Operations Horizon; FAC-014-3 – Establish and Communicate System Operating Limits; IRO-008-3 – Reliability Coordinator Operational Analyses and Real-time Assessments; PRC-023-5 – Transmission Relay Loadability | Implementation Plan; PRC-002-3 – Disturbance Monitoring and Reporting Requirements | Implementation Plan; PRC-026-2 -- Relay Performance During Stable Power Swings | Implementation Plan; TOP-001-6 – Transmission Operations
Oct. 1, 2024	EOP-012-1 – Extreme Cold Weather Preparedness and Operations (Requirements 1–2 effective 4/1/28; Requirement 4 effective 10/1/29)
April 1, 2026	CIP-003-9 – Cyber Security – Security Management Controls

Items Posted for Comment			
Posting	**Action**	**Start Date**	**End Date**
Project 2022-02 – Modifications to TPL-001 and MOD-032 | Draft 1 - MOD-032-2	Submit Comments	5/31/2023	7/14/2023
Project 2021-07 – Extreme Cold Weather Grid Operations, Preparedness, and Coordination - Phase 2 | D	Submit Comments	6/5/2023	7/20/2023
Project 2020-06 Verifications of Models and Data for Generators	Submit Comments	6/7/2023	7/21/2023

These effective dates can be found here.

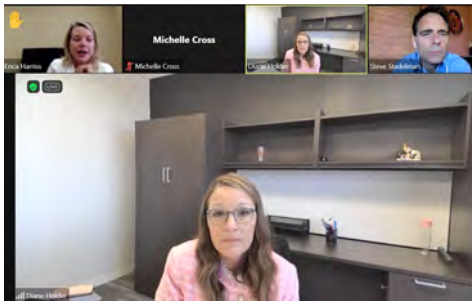
Update on Compliance Monitoring Engagements

Going forward, RF Compliance Monitoring engagements will be performed in Align and the Secure Evidence Locker. If you are in the process of an engagement currently being conducted in MKInsight, it will remain in MKInsight through the entire engagement process. We would like to thank all the entities that assisted us in the piloting phase of our Align implementation. This was a great collaboration between RF and entities throughout our footprint. Compliance Monitoring will be covering this and more at the upcoming Fall Workshop in Pittsburgh.

RF Testifies before the Illinois State Senate Committee

Grid reliability is RF's number one concern. RF's Vice President of Entity Engagement and Corporate Services Diane Holder and Director of Entity Engagement and External Affairs Brian Thiry testified before the Illinois State Senate Energy and Public Utilities Committee on reliabilty topics in April, in service of that mission.

RF is a resource states can call upon to remain well informed regarding key reliability topics as they craft policies for a cleaner, more sustainable grid. Continued collaboration, coordination and thoughtful action among NERC, the Regional Entities, and state and federal policymakers is necessary to successfully address the complex reliability challenges emerging as the grid is transformed.

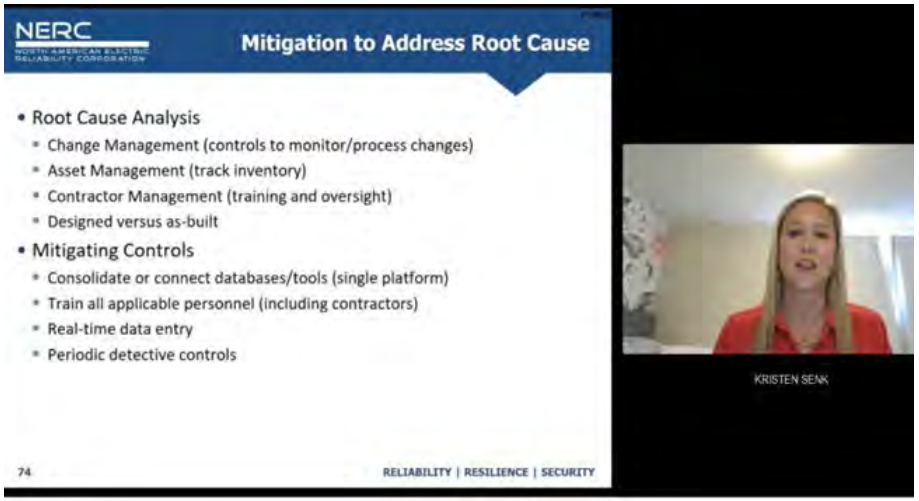


Diane Holder Participates in Panel at OPSI Spring Meeting

RF Vice President of Entity Engagement and Corporate Services Diane Holder (far right) participated in a panel focusing on "The Transition to Clean Energy: Can We Navigate Reliability Issues While Turning Away Coal?" at the 2023 OPSI Spring Meeting in Charleston, West Virginia, in April. Continuing to engage in these important conversations with states, RTOs and other stakeholders is a vital piece of the puzzle in navigating the grid transformation.

RF Participates in ERO Facility Ratings Webinar

At the ERO's Facility Ratings Management Webinar on May 24, Kristen Senk, RF's Director of Legal & Enforcement, shared with industry some facility ratings pitfalls, root causes, and mitigation trends observed by the RF team.



Tech Talk Recap:
April, May, June 2023

RF hosted three Tech Talks this quarter. Topics included:

- An overview of substation physical security practices by our manager of Entity Engagement, Mike Hughes, that can aid and enhance the reliability, security, and resilience of the Bulk Power System, followed by a discussion headed by enforcement attorney Mike Hattery about how to proactively approach physical security common failure points.
- An analysis of a South Australia Case Study on renewable integration and November 2022 Islanding Event, presented by Mark Thompson, Senior Engineer for AEMO, and Cathryn McDonald, Network Emergency Manager for SA Power Networks. The presentation provided an in-depth analysis of the wind event that resulted in islanding and high levels of renewable penetration to the grid as well as their approach to the great energy transition.
- An overview of the 2023 RF Summer Assessment by Tim Fryfogle, Principal Engineer, Engineering and System Performance, where he discussed resource adequacy, peak loads, risk conditions, mitigations, and the challenges that come with the summer season.
- A presentation on the value of EV managed charging to bulk power systems by National Renewable Energy Laboratory researcher Luke Lavin, who discussed the impact EVs have on resource aggregation as well as the costs EVs have to the bulk power system.

RF Publishes 2022 Annual Report

RF recently published its 2022 Annual Report. The report focuses on the following topics:

- Reviewing compliance and enforcement data to find trends and combat reliability risks.
- Resilience efforts and tools available for use against both physical and cyber-attacks on the grid.
- How the extreme cold weather events from 2021's Winter Storm Uri and 2022 Winter Storm Elliot underscore the importance of cold weather preparedness to the grid.
- Various organizational advancements and achievements including being named a 2022 Top Workplace by the Plain Dealer and Cleveland.com.

Click here to read the report.

RF Volunteers at Community Organizations in Cleveland

RF staff members gave back to the community in June, volunteering at the following Cleveland-area organizations:

- Shoes and Clothes for Kids
- Boys & Girls Club of Northeast Ohio
- Laura's Home Women's Crisis Center.

We are looking forward to the next opportunity to help our community!

2023 Protection and HP Workshops Register Today

Mark your calendars for the upcoming RF Protection System and Human Performance Workshops. We have opted for both of our workshops to be entirely virtual this year for easy access to all who wish to attend.

Annual Protection System Workshop for Technical Personnel

Aug. 2, 2023 | 1 - 5 p.m.

Register

This is a highly interactive workshop with the attendees providing ideas, suggestions, and stories for the benefit of everyone. This workshop will be entirely virtual this year.

Should you have any questions, please contact John Idzior or Thomas Teafatiller.

Annual Human Performance (HP) Workshop

Aug. 3, 2023 | 8 a.m. - 12 p.m.

Register

This event will focus on the practical application of HP 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. This workshop will be entirely virtual this year.

Should you have any questions, please contact John Idzior.

2023 Fall Workshop Sept. 26-27 in Pittsburgh

Register

Join us for the 2023 RF Fall Workshop in Pittsburgh, PA.

At this workshop, we'll highlight the importance of collaboration and partnerships for the electric industry amid the great energy transition as we look to build the grid of the future. We will delve into the grid's interdependencies and explore how working together can pave the way for a more reliable and sustainable energy landscape.

Our lineup of speakers includes representatives from state government, natural gas, cybersecurity, and water industries. They will share their insights, experiences, and innovative approaches to address the challenges and opportunities that lie ahead.

Secure your spot today by signing up. We look forward to welcoming you to the 2023 Fall Reliability Workshop and sharing an enriching experience with you.

Calendar of Events

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

Date	RF Upcoming Events
7-17-23	Technical Talk
8-2-23	Protection System Workshop
8-3-23	Human Performance Workshop
8-14-23	Technical Talk
8-23-23	Q3 Board of Directors Committee Meetings
8-24-23	Q3 Board of Directors Meeting

Industry Events

Date	Industry Upcoming Events
7-12-23	MISO Resource Adequacy Subcommittee
7-16-23	Seventh Meeting of the Joint Federal State Task Force on Electric Transmission
7-16-19-23	NARUC Summer Policy Summit
7-26-23	PJM Members Committee Meeting, Markets & Reliability Committee Meeting
7-27-23	FERC Open Meeting
8-10-23	Joint Technical Conference Regarding Physical Security of the Bulk Power System
8-17-23	NERC Board of Trustees Meeting
8-22-23	MISO Reliability Subcommittee, Resource Adequacy Subcommittee
8-23-23	PJM Special Members Committee Meeting on Resource Adequacy
9-10-23	PJM Members Committee Meeting, Markets & Reliability Committee Meeting

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
CENTERPOINT ENERGY
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
EXELON CORPORATION
FIRSTENERGY SERVICES COMPANY
HAZELTON GENERATION LLC
HOOSIER ENERGY RURAL ELECTRIC COOPERATIVE, INC
ILLINOIS CITIZENS UTILITY BOARD
ILLINOIS MUNICIPAL ELECTRIC AGENCY
INDIANAPOLIS POWER & LIGHT COMPANY
INTERNATIONAL TRANSMISSION COMPANY
LANSING BOARD OF WATER AND LIGHT
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
WABASH VALLEY POWER ASSOCIATION, INC
WISCONSIN ELECTRIC POWER COMPANY
WOLVERINE POWER SUPPLY COOPERATIVE, INC