RELIABILITY FIRST

Issue 4 | 2023 Q4

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

Note from the President

Dear Stakeholders,

Here we are in December wrapping up what's been another busy year! In February, we conducted our first-ever statewide security tabletop exercise, working with local utilities, health care, law enforcement, state and federal agencies, municipal government, telecommunications, and more to stress and test coordination, communication, and response, and I feel that it was a tremendous success. We also reached new audiences with the video we produced with NERC and NPCC on the 20-year anniversary of the 2003 Northeast Blackout in August. And we completed our largest ever number of on-site winterization visits at generating plants, part of a program we aim to continue to strengthen as we learn from the areas for improvement exposed by Winter Storm Elliott.

In the coming year, there are tremendous opportunities and responsibilities before us. We made great progress with our efforts to build relationships and share our expertise on reliability topics with state policymakers and commissioners, testifying at public hearings and giving presentations throughout the year. We are now in a position where policymakers think to call us, and we will continue to work with states to inform their policy decisions. Our focus has been to educate and inform about the trilemma of reliability, cost, and environment and about the trade-offs and issues associated with transitioning our grid at breakneck speed while demand is also increasing. This work will continue to be a major focus for us in 2024.

We will also be doing a lot of work related to NERC's Interregional Transfer Capability Study (ITCS), running analysis and communicating with industry, regional partners, NERC, and state and federal policymakers. The stakes are extremely high, and we cannot afford to do this wrong.

Lastly, I continue to remind you to remove and reduce today's risks while you can before unknown future risks crop up. Proactive participation in the NERC Standards process to address emerging risks is vital to ensuring a secure and reliable electric system.

Be safe, be well and happy holidays from everyone here at RF.

Forward Together,

Tim

Issue 4 | 2023 Q4

INSIDE THIS ISSUE

Follow us on:

From the Board

2023 Annual Meeting of Members and Q4 Board Meeting Recap

U.S. Senator
John Hickenlooper

RF held its 2023 Annual Meeting of Members and Q4 Board Meeting on Dec. 7 in Washington, D.C. Attendees heard from U.S. Sen. John Hickenlooper of Colorado as the keynote speaker, who emphasized the importance of maintaining reliability amid the great energy transition, and noted the Bipartisan Infrastructure Bill as one of the tools in place to support these efforts.

Chairman
Emile Thompson

Chairman Emile Thompson of the Public Service Commission of the District of Columbia also joined the meeting as a guest speaker. He detailed the mission and goals of his organization and shared that Washington, D.C., is focusing on addressing the risk profiles in NERC's 2023 ERO Reliability Risk Priorities Report, including energy policy, grid transformation, security risks and critical infrastructure interdependencies. He also emphasized the Public Service Commission's strategic investment in resilience and highlighted recent projects.

Patrick Cass
Independent

Courtney Geduldig, chair of the RF Nominating and Governance Committee, presided over the independent director election, where incumbent director Patrick Cass was elected to serve a fourth term through December 2025. Mr. Cass has been a valued member of the RF Board since 2014 and will continue serving as the lead independent director and chair of the Finance and Audit Committee. Finally, RF Senior Director of Corporate Services Beth Dowdell provided an overview of the company's financial position, including a review of the third quarter financial numbers and projections for the company to end the year within budget.

The Q4 Board Meeting also featured several special guests, including keynote speaker Manny Cancel, senior vice president at NERC and chief executive officer of the E-ISAC. He was joined by Deputy Director Erik Vanderberg of the Office of Electric Reliability, who provided FERC updates, and Heather Polzin, attorney advisor and reliability coordinator for the Office of Enforcement, and David Huff, electrical engineer for the Office of Electric Reliability, who provided a summary of the FERC-NERC Winter Storm Elliott Report.

Continuous Improvement

By Sam Ciccone, Principal Reliability Consultant, Entity Engagement

Value Stream Mapping

The Journey to Security, Resiliency and Reliability

Every year children around the world wait impatiently for the arrival of Santa to leave them all the wonderful gifts they wished for. Santa and his elves have a year to prepare for that one magical night to fulfill children's hopes and dreams of the newest video game console, the latest tablet, or even the classic Red Ryder Carbine Action 200-shot Range Model air rifle - just don't shoot your eye out! But as the world grows by millions of people each year, it is important for Santa and his elves to look at the process and see where inefficiencies can be reduced to ensure continued timely delivery of toys around the world. This type of analysis might look something like this.

Much like Santa having to deal with more complexity in the world, organizations from all industries should continuously adjust their processes to ensure they deliver high quality products efficiently. In our industry, examples include: how can you reduce the time it takes to prepare for an audit? Or, how can efficiencies be realized when you implement programs such as vegetation management or protection equipment maintenance? Value Stream Mapping is one way to improve any process, just like in the Santa's Workshop example linked above.

What is a Value Stream Map?

A Value Stream Map (VSM) is a tool used to visualize a process in enough detail to uncover where waste exists, how much time each process step takes to complete, the number of resources needed to complete the process, and much more. It is rooted in the Continuous Improvement (CI) concept of Lean Six Sigma which is an improvement philosophy that values proactively preventing defects over detecting them after the fact and promotes standardizing work processes to reduce wasted time, according to the American Society for Quality. VSMs "facilitate clear communication and collaboration, encourage continuous improvement of a process, and enable culture change within an organization," according to an article by Purdue University. The focus is on increasing value-added steps and reducing non-value-added steps. Non-value-added time accounts for almost 50% of total time in many processes, according to Villanova professor Tina Agustiady.

To improve a process using a VSM, the first step is to depict the current state. Holding a Kaizen Event with an impartial facilitator usually works well when developing the VSM. This activity involves holding a brainstorming session focused on improving an existing process. You should include all the stakeholders of the process, set up one or more sheets of paper across a wall to give yourself enough room to properly draw out the process, and have a stack of sticky notes on which to write all the steps. You want to go from left to right, starting with the first step and working your way to the last step, while collaborating and having discussions throughout the event. You need to think about how long each step takes. You can come up with an educated guess based on experience, or if possible, you can also use employee timesheets to get a representation of the time associated with different activities. You need to know the number of personnel involved in the process, and the results of the current state may show not only waste that needs to be eliminated but a need for more, or less, personnel.

Analyze the Current State

Once your current state is depicted, then it is time to analyze the process. Where are areas of waste, a common one being waiting (e.g., a compliance department waiting for an SME to provide you with the needed compliance documentation)? You can identify steps that may be taking longer than they should and if they can be shortened. What are the bottlenecks and dependencies on external parties? In what areas do we need more resources, or can we maintain productivity with less resources?

This is also the time to get management that is already familiar with

Continued on page 6

Continuous Improvement

Continued from page 4

the process involved in analyzing the current state. They should review your VSM and assign numerical values for the steps, e.g., 9 for the "must have" value-added step, down to a 3 or 1 for those non-value-added steps. This will help measure the value of each step in the process.

Create the Future State

What do you want the process to look like, for example, when you want to reduce the time to get all the required documentation for a NERC compliance audit? Is there a system you can incorporate that makes this step more efficient, such as implementing a new database or replacing the current database for more efficient communication among departments? How can you improve how compliance evidence is stored and updated, including a quick feedback loop and request for information feature?

Maybe there are steps you need to add to make the process more robust – it's not always just about removing steps and reducing time – it's about value. Your protection equipment maintenance process may show the need for change to add critical steps, such as ensuring a relay is put back into service the way it was before testing and maintenance, adding safety instructions you may have uncovered from previous lessons learned, or adding steps to have another worker double-check that all testing requirements of NERC standard PRC-005 have been met.

You can also use a VSM to identify the need for internal controls. Internal controls can add value to any process. One example of a process that can be improved using controls is patch management required by CIP-007-6 R2. If you mapped out and analyzed the current state of your patch management process, you may see that integrating controls could help create an improved future state. For example, adding a verification control where a secondary person reviews and approves the patch testing outcome to ensure accuracy before installation and validation could catch potential issues earlier in the process and save time overall. The future state, when implemented, is not the end of the process. It should be periodically reviewed due to changing conditions, hence the overall objective of continuous improvement.

We practice what we preach. And we can help!

The RF Entity Engagement group uses VSMs to see all the process steps within our core and project work, one example being the Assist Visit process. Although we start with the visualization like any VSM development, we customized it by transferring it to a spreadsheet that suits our purposes as a service organization and that includes cycle time calculations and how much we are utilizing our human resources.

We have several staff members who are trained in facilitation techniques in accordance with the International Association of Facilitators (IAF) through our RF Facilitation Community of Practice where members collaborate, learn, and practice facilitation techniques. This allows RF the ability to help entities develop a VSM and assist with a variety of other issues. If you'd like us to help you improve your process using VSMs, please contact us.

Thank you all for what you do to keep our grid secure, resilient, and reliable. Whether you celebrate Hanukkah, Kwanzaa, Christmas, or any other holiday this winter season, I wish a safe and happy holiday to all of you!

VSM Resources

The following are resources that provide more details about Value Stream Maps. They may include VSM examples with much more detail than you need for your process, so you can customize the VSM to your needs.

Value Stream Mapping:

- *How to Visualize Work and Align Leadership for Organizational Transformation: Book*
- *Mindtools: Value Stream Mapping*
- *American Society for Quality (ASQ): What is Value Stream Mapping (VSM)?*
- *A Lean Journey: Five Simple Ways to Make Your VSM A Valuable Improvement Tool*

2023 Long-Term Resource Assessment

RF performs an annual assessment to ensure that its footprint has adequate resources to serve anticipated load demand for the next 10-year period. Each assessment area within RF (i.e., PJM and MISO) has a targeted reserve margin level, which identifies the minimum number of resources needed to meet a loss of load expectation (LOLE) of one day in 10 years. The results of this assessment express each area's ability to meet the targeted reserve margin level. RF developed this assessment collaboratively with data provided from both PJM and MISO. This article will share some highlights from this assessment.

Key Findings

- PJM is projected to have a 0.81% load growth rate over the next 10 years and will meet its target reserve margin requirement of approximately 15%, which includes both Existing-Certain and Tier 1 resources.
- MISO is projected to average a 0.42% load growth rate from 2024 through 2033.
- The MISO target reserve margin, which includes both Existing-Certain and Tier 1 resources, is projected to not satisfy its reserve margin target starting in 2028 and continuing for the rest of the 10-year period. The largest reserve margin deficit was identified in 2032, which was 19,255 MW below the target reserve margin.
- MISO transitioned to its first year of seasonal Capacity Auctions (summer, fall, winter, spring). The switch to a seasonal construct now highlights non-summer risk, but it also derives seasonal accreditation and seasonal resource adequacy requirements.
- Drivers of the increase in the MISO Reserve Margin requirement are electric demand, particularly the demand in electric vehicles, and an increase in intermittent resources.

PJM

Capacity and Reserve Margin

PJM resources are projected to be 198,695 MW in 2024 and increase to 271,139 MW by the end of 2033. The resource calculations include planned generation retirements, planned generation additions and changes, and an addition of 50% of the Tier 2 projects presently listed in the generation interconnection queue.

The left-side figure on the following page shows the reserve margin for PJM from 2024 through 2033. Please note that varying resource scenarios are used to gauge how much of the generation queue (i.e., generation that is yet to be built) is needed to stay above the target reserve margin. The blue line represents PJM's reserve margin with both Existing-Certain and all Tier 1 resources. On average, PJM has a 34% reserve margin and is expected to meet and significantly exceed its target reserve margin (of approximately 15%) from 2024 through 2033.

Peak Demand

The right-side figure on the following page displays actual demand data with a 10-year forecast of demand for PJM. PJM's 10-year forecasted growth indicates that peak demand has steadily increased over time. Based on the latest 2023 forecast, PJM is projected to average a 0.81% load growth per year over the next 10 years. The PJM summer peak demand in 2024 is projected to be 149,737 MW and increase to 160,971 MW in 2033 for total internal demand (TID). Annualized 10-year growth rates for individual PJM transmission zones range from -0.3% in Commonwealth Edison Company to 2.2% in Virginia Electric and Power Company.

Frequently Used Terms

Existing-Certain: Includes operable capacity expected to be available to serve load during the peak hour with firm transmission.

Tier 1: Includes capacity that is either under construction or has met all the required milestones for interconnection.

Tier 2: Includes capacity that has requested an interconnection but has not met some required milestones or executed certain agreements.

Tier 3: Other planned capacity that does not meet the requirements of Tier 1 and Tier 2.

Confirmed Retirements: Capacity with formalized and approved plans to retire. Please note that generator retirements are evaluated on a case-by-case basis by PJM and MISO for potential reliability impacts. If it is determined that reliability impacts exist, the Generation Owner is requested to defer retirement until the reliability impacts are addressed. In this assessment, all confirmed generator retirements are assumed to occur after any reliability concerns are addressed.

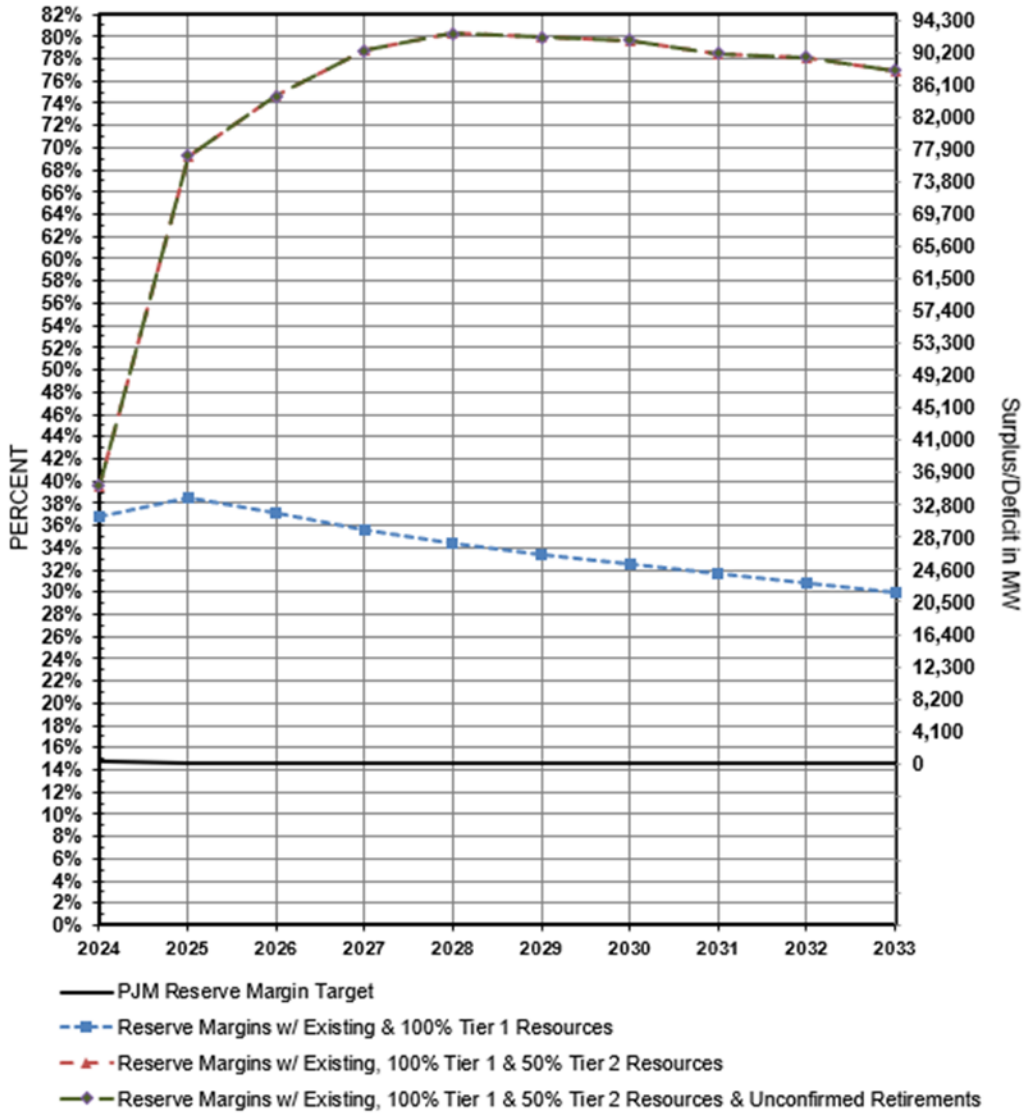
Unconfirmed Retirements: Capacity that is considered likely to retire by resource owners, but the formal notification has not been submitted to the respective party. Also included are units for which such notice has been made, but a reliability impact assessment or mitigation is pending.

Continued on page 7

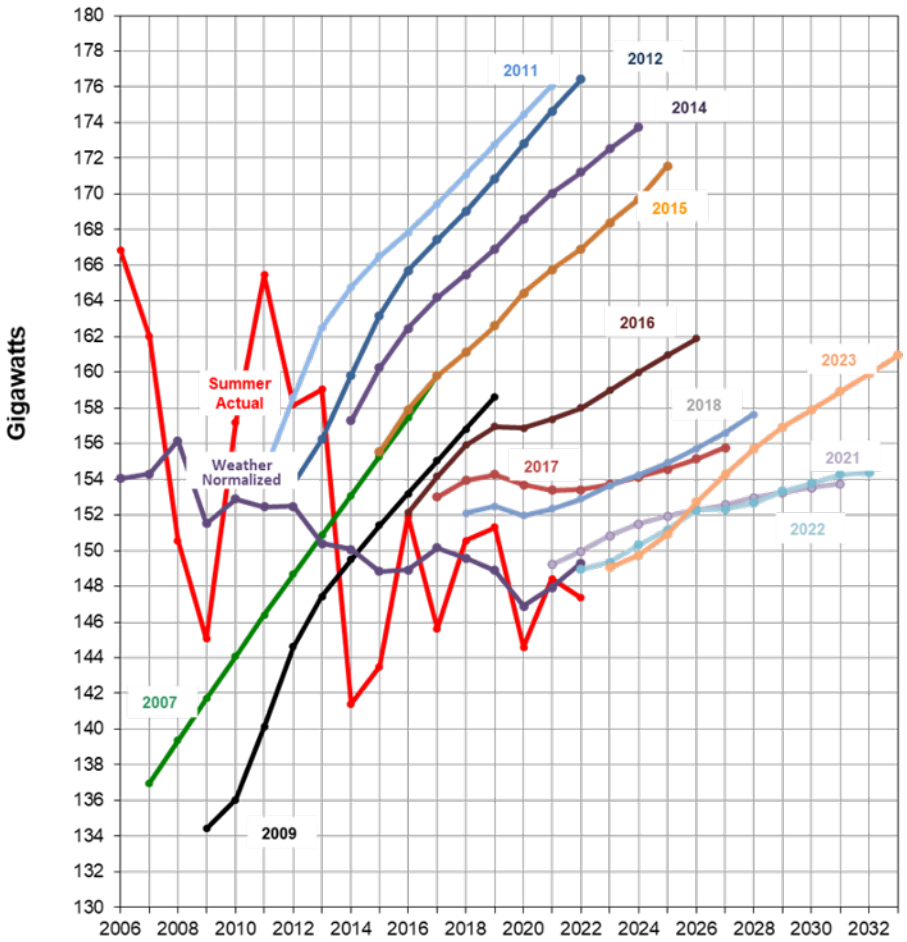
2023 Long-Term Resource Assessment

Continued from page 6

PJM RTO Summer Reserve Margin Projections 2024 - 2033



PJM RTO Peak Demand Data Actual 2006 - 2022 Select 10 Year TID Forecasts Through 2033



2011 Includes the expansion of the PJM RTO footprint with First Energy (ATSI) and Duke Energy Ohio and Kentucky
2013 Includes the expansion of the PJM RTO footprint with East Kentucky Power Cooperative
2019 Includes the expansion of the PJM RTO footprint with Ohio Valley Electric Cooperative

Continued on page 8

2023 Long-Term Resource Assessment

Continued from page 7

MISO

Capacity and Reserve Margin

MISO resources are projected to be 146,823 MW in 2024 and then increase to 149,011 MW by the end of 2033. This resource calculation includes planned generation retirements, planned generation additions and changes, and Tier 2 and Tier 3 projects from the generation interconnection queue.

Coal and nuclear availability to provide resource adequacy contributions has declined by 300 MW and 140 MW respectively. This is mainly due to retirements but it is not as large as projected last year due to delayed retirements. New wind and wind accreditation increased 725 MW, and solar and solar accreditation increased 920 MW. Natural gas additions to meet resource adequacy requirements in MISO went up by 4 GW.

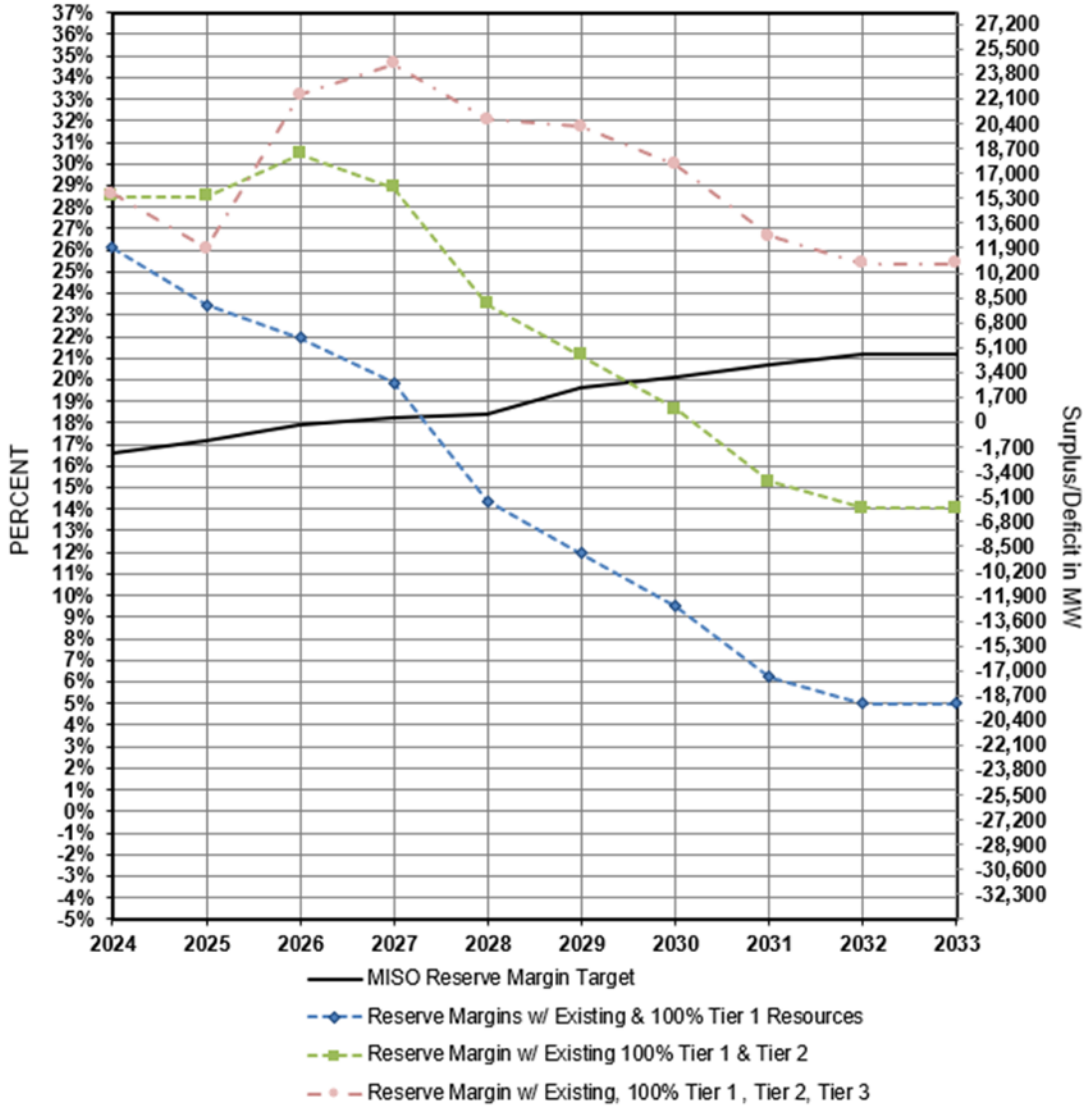
There are over 49 GW of generation installed capacity (predominantly solar) with signed generation interconnection agreements in MISO that are projected to come online within the next five years. Some projects have experienced delays in achieving commercial operation due to supply chain issues, even as late as the post-agreement phase. MISO tariff changes and interconnection queue processes are reducing interconnection queue timelines.

Recognizing that many projects for new generation terminate the interconnection process before completion, MISO applies a factor to the Tier 2 and Tier 3 resource capacities based on the study phase and likelihood of resources coming online.

The effect is to reduce the capacity of prospective new resources for more accuracy in long-term planning by accounting for the uncertainty and delays of new resources completing the interconnection process.

The figure to the right shows the reserve margin for MISO from 2024 through 2033. Please note that varying resource scenarios are used to gauge how much of the generation

MISO RTO
Summer Reserve Margin Projections
2024 - 2033



Continued on page 9

2023 Long-Term Resource Assessment

Continued from page 8

queue (i.e., generation that is yet to be built) is needed to stay above the target reserve margin.

MISO's anticipated reserve margin, which includes Existing-Certain and all Tier 1 resources, does not satisfy the target for 2028.

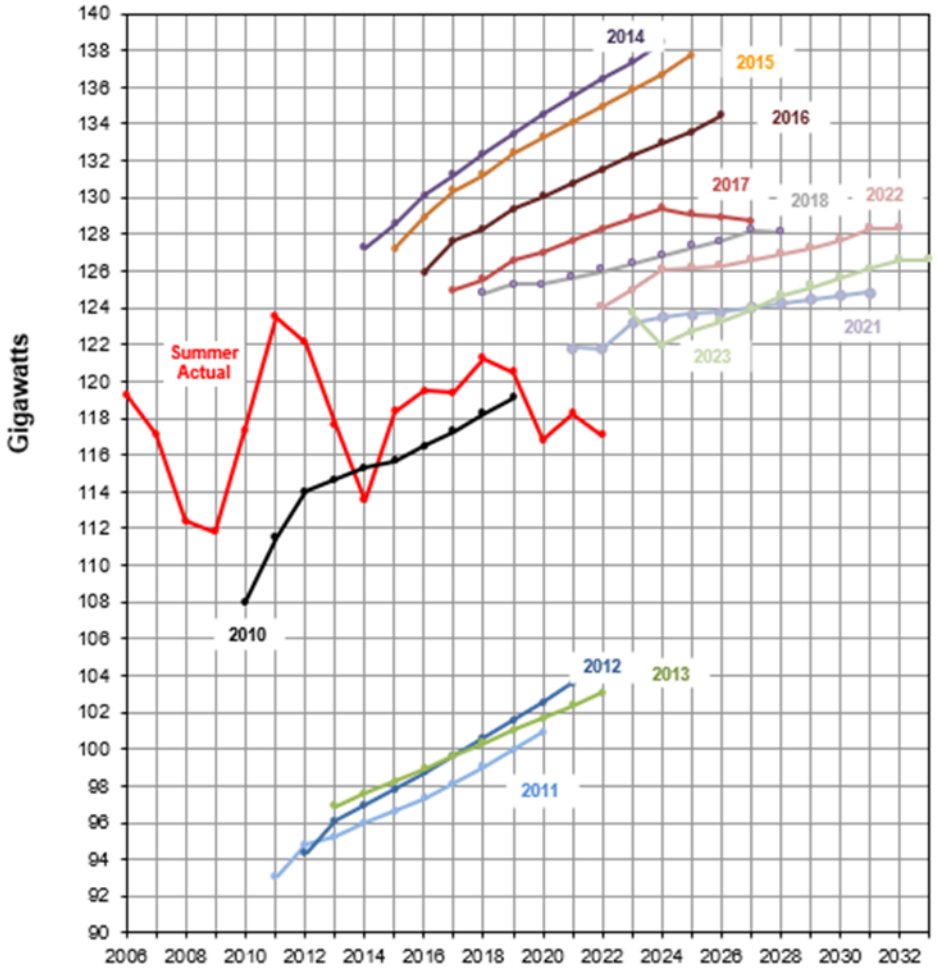
The MISO anticipated reserve margin projected for 2028 is 4,729 MW below the reserve margin target. Continuing in 2029, the projected reserve margin is 8,987 MW below the target and continues to decline to 19,255 MW below the target in 2033. These values are represented in the figure on the previous page with the blue line.

Peak Demand

The figure to the right displays actual demand data with a 10-year forecast of demand for MISO. MISO's 10-year forecasted growth indicates that peak demand has steadily increased over time.The projected MISO annual load growth rate for 2024 through 2033 is approximately 0.42%.

The MISO summer peak demand is projected to be 121,933 MW in 2024 and 126,593 MW in 2033 for total internal demand (TID).

MISO RTO Peak Demand Data
Actual 2006 - 2022
Select 10 Year TID Forecasts Through 2033



2011 Includes the reduction of the MISO RTO footprint with First Energy (ATSI), Cleveland Public Power and Duke Energy Ohio and Kentucky moving to PJM RTO
2014 Includes the expansion of MISO RTO footprint with MISO South

Winter 2023-2024 Reliability Assessment

Reliability Resource Risk Assessment

RF annually performs a seasonal winter reliability assessment to ensure that its footprint has adequate resources to serve anticipated demand. This assessment is comprised of two distinct types of analysis for each assessment area, PJM and MISO, which are defined below.

1. Capacity and Reserve Analysis – this is a review of additional capacity resources, called Planning Reserve Margin, compared to the resources needed to meet a loss of load expectation of one day in 10 years, called the Reserve Margin Requirement.
2. Random Generator Outage Risk Analysis – this is a review of the potential for large amounts of resource unavailability combined with expected and higher than anticipated demand (associated with historical worst-case scenarios).

RF developed this assessment collaboratively with data provided from both PJM and MISO. This article shares some highlights from the analysis.

Capacity and Reserves Analysis

For the upcoming winter of 2023-2024, both MISO and PJM are expected to have adequate resources to satisfy their respective Reserve Margin Requirements.

- However, if the upcoming winter experiences a higher than anticipated number of resource outages, there is a likelihood that PJM and MISO areas will need to utilize operating measures to serve forecasted load demand and maintain reliability. These operating measures include Load Modifying Resources, non-firm transfers into the system, and energy-only interconnection service resources not receiving capacity credit.
- Note that this risk increases in probability when the forecasted load demand for the 2023-2024 winter is higher than expected.
- In addition to these operating measures, MISO has additional resources in the southern portion of its footprint that can be called upon for increased internal transfers. This step could be considered in case of emergency only, as it would mean exceeding the Sub-Regional Import/Export Constraint between the MISO North/Central and South regions.
- The resource outage risk assessment, outlined below, further assesses the capability of both MISO and PJM to meet their anticipated load demand under random resource outage scenarios based on actual Generator Availability Data System (GADS) outage data.

Additional factors

Reliable operation of the thermal generating fleet is critical to winter reliability. That, coupled with assuring adequate fuel supplies, are ongoing winter reliability concerns. Present domestic and global affairs warrant even greater attention on generator fuel supplies, including natural gas, fuel oil, and coal, for the upcoming winter.

While many factors that contributed to uncertain rail shipment of coal to electric generators prior to the 2022-23 Winter Resource Reliability Risk Assessment have subsided, other transport issues have emerged for this winter. Drought conditions impacting the Missouri River and other major navigable rivers could restrict coal availability and cause units to run at a derated level to conserve coal inventory. Low water levels can also affect generators that rely on once-through cooling processes by limiting the generator's capacity output. Careful attention to periodic fuel surveys is needed to provide early indication of fuel supply risks.

PJM Capacity and Reserves

Net capacity Resources [1]	178,188 MW
Projected Peak Reserves	50,710 MW
Net Internal Demand (NID)	127,478 MW
Planning Reserve Margin	39.8%

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

Continued on page 11

Winter 2023-2024 Reliability Assessment

Continued from page 10

The PJM forecast Planning Reserve Margin of 39.8% is greater than the 27% Reserve Margin Requirement for the 2023 planning year. However, the Planning Reserve Margin for this winter is lower than the 2022 forecast level of 45.9%. This is due to a decrease in existing certain generation and the increase in Net Internal Demand (NID). Based on the numbers provided, under expected operating conditions PJM will satisfy its reserve margin requirement.

MISO Capacity and Reserves

The MISO forecast Planning Reserve Margin of 55.8% is greater than their Reserve Margin Requirement of 25.5% for the 2023 planning year. The Planning Reserve Margin for this winter is higher than the 2023 forecast level of 43.1%.

Net Capacity Resources	147,097 MW
Projected Peak Reserves	52,703 MW
Net Internal Demand (NID)	94,394 MW
Planning Reserve Margin	55.8%

MISO has filed and implemented a seasonal resource adequacy construct and seasonal unit accreditation to better affirm adequate supply in all seasons. As a result, MISO has raised Reserve Margin Requirement levels for the 2023-24 Winter season. The 2023-2024 Planning Resource Auction conducted in April 2023 was the first implemented under the seasonal construct.

With the transition to seasonal capacity auctions, shifting risk across the seasons appropriately and seasonal accreditation, MISO is projecting sufficient capacity margins in excess of the reserve margin requirements for this winter season.

RF Footprint Resources

Since both PJM and MISO projections have adequate resources to satisfy their respective forecasted Planning Reserve Margin requirements, the RF region is projected to have sufficient resources for the 2023-2024 winter period.

Random Generator Outage Risk Analysis

The following analysis evaluates the risk associated with planned and random forced generation resource outages that may reduce the available capacity resources to a level that is below the load demand obligations of both PJM and MISO. Reports and/or other data released by PJM, MISO and NERC for this same period may differ from the data reported in this assessment due to different assumptions that were made by RF.

Net Capacity Resources	195,083 MW
Projected Peak Reserves	60,718 MW
Net Internal Demand (NID)	134,365 MW
Total Internal Demand (TID)	141,738 MW

This analysis differs from NERC's in that RF uses actual historical GADS data from a rolling five-year period, which provides a range of outages that occur during the winter period.

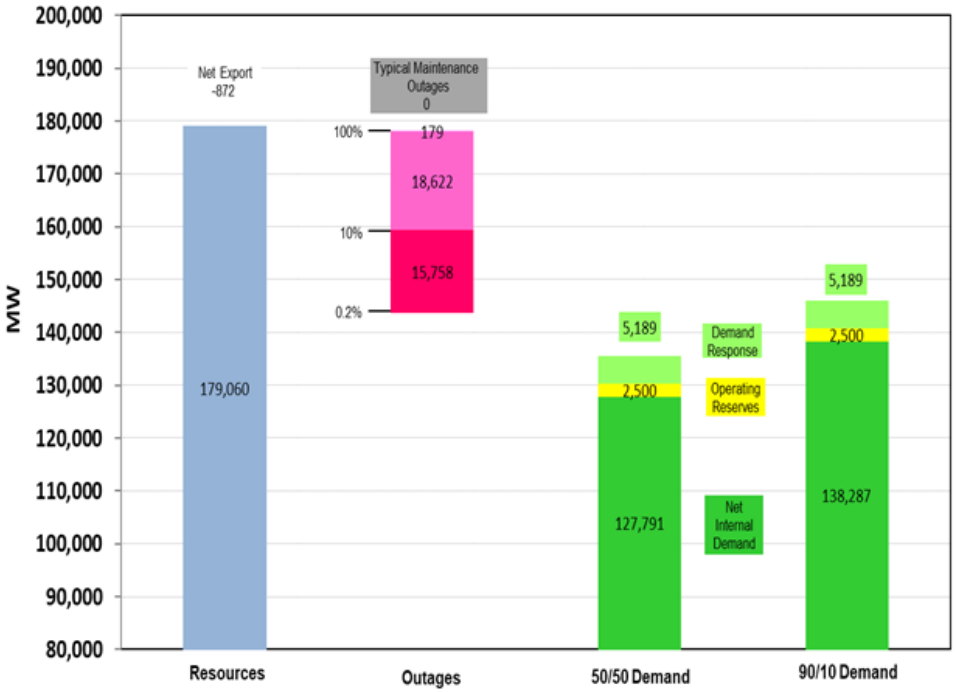
RF created a Resource Availability Risk Chart for both PJM and MISO based on the anticipated conditions for the upcoming 2023-2024 winter

Continued on page 12

Winter 2023-2024 Reliability Assessment

Continued from page 11

Exhibit 1 - 2023/2024 Winter PJM Resource Availability Risk Chart



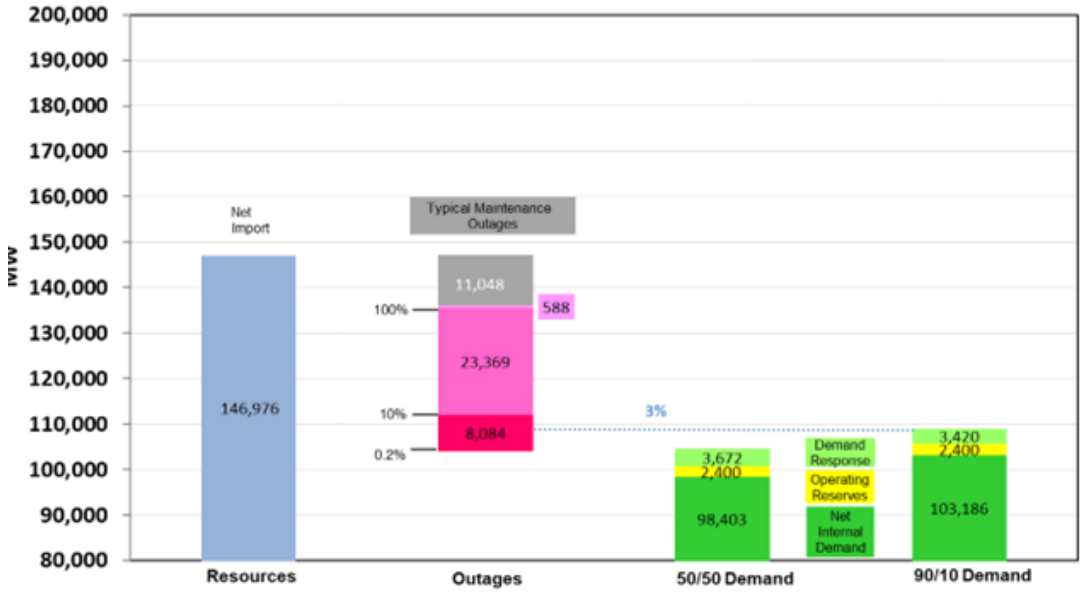
season[1]. The intent of these charts is to identify potential risks with having enough resources[2] available to serve demand.

A risk indicator from the charts is when the Outages[3] (gray and red tinted bars) overlap with Demand (green and yellow bars). Outages are presented as a probability[4] of occurrence. This risk will likely result in conservative operations, initiation of Load Modifying Resources/Demand Response programs, and/or utilization of operating reserves. In the event that utilization of all Demand Response is not sufficient to balance resources with demand, system operators may first reduce operating reserves prior to interrupting firm load.

In Exhibit 1 for PJM, there is a minimal risk that the amount of outages would require Demand Response for both the 50/50 and the 90/10 demand forecast for the upcoming winter.

In Exhibit 2 for MISO,there is a 3% probability that Demand Response will be required during high demand (90/10 demand).

Exhibit 2 - 2023/2024 Winter MISO Resource Availability Risk Chart



[1]Winter constitutes the months of December, January, and February.

[2]Resources 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 area's reserve margin requirement.

[3]Outages include planned maintenance outages (gray bar) and random forced outages (red tinted bar).

[4]Probability 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 winter periods that would have exceeded the reserve margin that is listed.

Information Security

By Erik Johnson, Director of Reliability Analysis

'Changes aren't permanent, but change is': Adaptability is crucial to keep up with the evolving world of information security

This article was originally published in November in CXO Tech Magazine.

In the world of information security, we have talked about the increasing pace of change for the last 25 years. And rightfully so – even the landscape of threat actors has seen a significant transformation over time. Initially, cyber-attacks were primarily the domain of nation-states, used as a digital weapon to further their geopolitical interests. Then, a new breed of cyber attackers emerged – "hacktivists."

These individuals or groups leveraged cyber-attacks as a form of protest or to advocate for a cause. Recently, we've seen a convergence of these two distinct domains. State-sponsored hacktivists have begun to appear, blurring the lines between government-led and citizen-led attacks. This evolution has added another layer of complexity to the cybersecurity landscape, making it more challenging to attribute attacks and defend against them. We have adapted quickly in some areas and not at all in others.

This ever-changing threat landscape brings to mind the lyric "changes aren't permanent, but change is," from the Rush song "Tom Sawyer." In the rapidly evolving world of information security, keeping pace with change is not just an option, but a necessity. Traditional security programs, often characterized by set patterns and predictable responses, are increasingly proving inadequate in the face of sophisticated and ever-changing cyber threats.

To meet this challenge, we must think differently about approaches we have become comfortable with to catch up with the pace of change. Removing unintended patterns and adopting a more dynamic, adaptive approach can enhance the effectiveness of your information security program.

Patching is one area where our approach may be out of date. Just like bell bottom jeans or mainframes, some things go out of style. Typically, we wait for a patch to be published before considering action and even judge our key performance indicators by how successfully we have met the required patch date. The problem is that we are at the mercy of the patch source, and the vulnerability often existed long before patch publication.

So, what can be done? Most security standards, regardless of origin (NERC, NIST, PCI-DSS, COBIT, ISO, etc.), allow the end user to define a comprehensive approach. A comprehensive policy should define items, such as mitigating controls, depending on the variable risk level to which a company is exposed. Think DefCon 5, 4, 3, 2, 1.

Consider assigning variably more robust security controls, such as a predetermined firewall rule set based on the DefCon example above, more rigorous security information and event management (SIEM) rules, and/or redefining trust boundaries and multi-layer validation for external data, based on the current risk level.

Let's move the discussion higher up to change control in general. If I asked you what your standard change control window was, you'd probably know it because it has not changed in years. This is another area where we are comfortable in the pattern we have set up, but those trying to get into your systems know it, too, because of that pattern. Adjusting your change control window to throw off attackers looking for the pattern could be done at whatever interval your organization deems appropriate.

This adjustment could also be done differently for different systems

Continued on page 14

Information Security

Continued from 13

based on criticality or a predetermined risk level. Obviously, the latter approach would require significantly more communication to implement. Instituting variable controls such as these creates the adaptive environment that is required today.

Let's be clear – I am not suggesting that if you implement these ideas in your environment, you will be set. They are just examples to point out that we often get comfortable in our patterns and don't see that while they address some risks now, they also bring in other risks as the environment around them evolves. Our adversaries can be aware of our patterns and leverage them against us, putting us in reaction mode.

By reviewing your existing environment for unintended patterns, you can enhance the benefits of the layered security you have already implemented. This can include improved security by introducing unpredictability into the system, making it harder for malicious actors to anticipate the system's responses. This unpredictability can deter potential attacks, as it increases the complexity and risk for attackers. Additionally, it encourages a more proactive and dynamic approach to security instead of a static one based on predictable patterns.

This can lead to the early detection and mitigation of threats, improving the system's overall resilience. Finally, removing patterns can promote continuous learning and adaptation within the security program, ensuring it stays effective despite evolving threats.

The dynamic nature of today's cyber threats necessitates a shift from traditional, pattern-based security programs to a more adaptive, risk-based approach. By identifying and changing predictable patterns in your security program, you can introduce an element of unpredictability that can deter potential attacks and enhance your system's resilience.

Remember, in the ever-evolving landscape of cyber threats, adaptability is key. So, take the first step today – identify those patterns and embrace change. Your security program will be all the better for it.

Internal Controls

By Courtney Fasca, Technical Auditor, Operations & Planning

Making a list and checking it twice: Internal controls reminders for the winter season

As we enter the holiday season, the signs of winter are making themselves more apparent everywhere. At home you may be shopping for loved ones, exploring decorative lights shows, or planning a family gathering, while at work it's time to prepare your facilities and equipment to perform during cold temperatures.

You may be applying heat trace to your outdoor equipment, testing your low temperature alarm systems in order to take action before equipment freezes, or identifying critical transmitters and insulating them in O'Brien boxes. These are all not only signs of winter and winterization prep, but they're also signs of your internal controls!

Internal controls are more than just evidence to share with the audit team. They help your organization to detect potential issues, prevent known issues, and correct issues that have occurred in a reasonable timeframe. Like the examples listed above, they are designed to prepare equipment to get through colder winter weather, and in doing so show auditors you are working to mitigate your risk.

When it comes to your internal controls, they should be well documented, tested, and implemented. Your controls are the tools your staff actively leverages to ensure continued reliability. Bringing awareness through training on your internal controls allows visibility across your organization (also consider ways to implement a feedback loop for suggestions of additional controls).

Training should not end with your staff. A common theme we have noticed on several engagements is the heavy reliance on contractors and using the work of others. A key point to using contractors – while you are paying them for their knowledge and expertise, you still need to check their work.

Are your contractors familiar with your winterization plans? If your contractors are in charge of putting down salt or removing ice from walkways, are the critical walkways identified and prioritized? If your contractor suggests an additional project or protection measure, is there a process in place to review those suggestions and ensure prompt follow-up? Internal controls not only help internally, but they can help guide external communication and coordination – again, to ensure continued reliability.

So, when you get your notification packet for your next engagement, just remember – by training your staff and contractors on what you do, designing and implementing internal controls to address risks, and documenting it all – you'll be taking steps to improve reliability and you'll be able to show the audit team your progress and get feedback (maybe even a Positive Observation).

If you're wondering where to start, please feel free to reach out to our Entity Engagement team for an Assist Visit with any questions or to ask about our Winterization Assist Visit options. Remember: even Santa adopted internal controls by always checking his list twice!

The Lighthouse

By Lew Folkerth, Principal Reliability Consultant, External Affairs

Executive briefing: The role of the executive in CIP compliance

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, resilience 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.

Background on the NERC CIP Standards

The Critical Infrastructure Protection (CIP) standards are part of the NERC Reliability Standards that are mandatory and enforceable for organizations that have an impact on the reliability of the Bulk Power System in North America. The CIP standards set a performance baseline for cyber and physical security for your operational systems. Your organization must meet, and is encouraged to exceed, this baseline.

Operational systems are those systems that control physical assets such as substations and generating plants. They are also the systems that will balance generation with load and ensure the Bulk Power System is operated reliably.

Security is not an end state, it is a set of processes that must be performed to reduce the security risk to an acceptable level. Similarly, compliance is a set of processes that ensure the security processes are performed in a consistent, effective, and timely manner.

Cheboygan Crib Lights, Cheboygan, MI – Photo: Lew Folkerth

Your role as an executive is to select a model to use for addressing cyber and physical security risk and the organizational structure you will use to address that risk. You will also select and support a CIP senior manager who will have the task of implementing and managing the selected structure.

Select a risk model and organizational structure

To start, I suggest organizing your thinking about security risk into three general categories:

- **Business risk** is the risk to the organization, which should include risks to finance, reputation, and staff retention.
- **Compliance risk** is the risk of being found in violation of the NERC Reliability Standards.
- **Security risk** is the risk of compromise or damage to cyber or physical assets.

One of the key differences between the NERC Reliability Standards and other types of standards is the mandatory and enforceable

Continued on page 17

Continued from page 16

nature of the NERC Reliability Standards with financial penalties for violations. The possible financial penalties serve to directly transfer compliance risk to business risk. This is shown in the organizational figures that follow, where compliance risk always impacts business risk.

In my tenure as a CIP auditor and an outreach team member, embedded at times in companies that needed major improvements to their security posture, some highly effective organizations have distinguished themselves. Let's look at some simple models for these organizations and see how they treat risk.

Figure 1 shows the Security group and the Compliance group managed separately. This is also known as a "siloed" approach, where the Security and Compliance groups are in their own silos. The intent of this form of organization may be to have each silo working cooperatively with the other, but in practice this frequently results in a disconnect between the Security and Compliance groups, with less than optimal results from each group.

Figure 2 would seem to be the natural order of an organization, where the Security group is foremost and the Compliance group takes a back seat. However, this form of organization can result in compliance being a bolt-on afterthought to security.

The organizations in both Figure 1 and Figure 2 can result in the Compliance group having insufficient information to demonstrate compliance to the CIP Standards. Also note that in both of the above figures, the Compliance group has no operational duties and is therefore primarily overhead. The next figure explores an organization where compliance adds value to the operation.

Figure 3 shows a type of organization I recommend, where compliance is used as a governance layer for security. In this organization, the Compliance group uses internal controls for governance of security functions. This organization does not make security less important, rather it takes the evidence collection and audit responsibilities off the security staff and places them on the compliance staff. This frees up the security staff to better manage security.

Select your CIP senior manager

The selection of a CIP Senior Manager is an important action. Here are a few thoughts to consider when you make this selection.

The CIP senior manager is a role defined by the CIP standards (see sidebar).

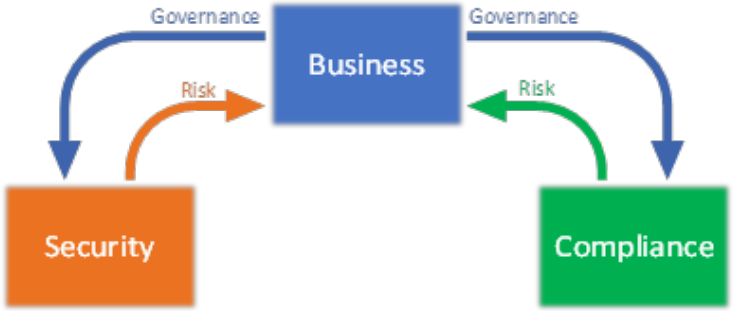


Figure 1 - Separation of Security and Compliance

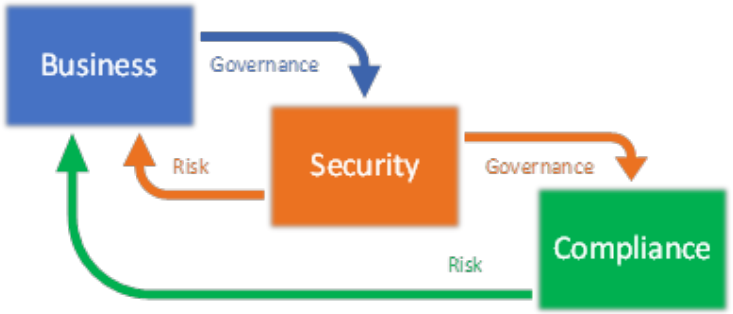


Figure 2 - Security as Governance for Compliance

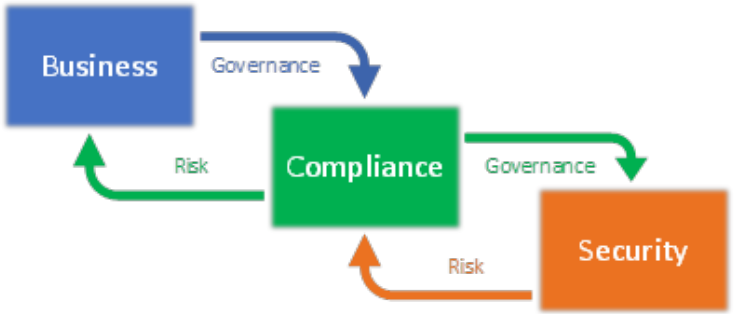


Figure 3 - Compliance as Governance for Security

Continued on page 18

Continued from page 17

CIP Senior Manager

A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP-002 through CIP-011.

From *"Glossary of Terms Used in NERC Reliability Standards"*

Simply stated, the CIP senior manager is the person you task with ensuring the CIP standards are applied to your operational systems. You can think of the CIP senior manager as the equivalent of a chief information security officer, but for operational assets rather than information assets.

The CIP senior manager is your eyes and ears into the CIP program and should be your liaison to the Security and Compliance groups. This means the CIP senior manager should understand both security issues and compliance issues and be able to communicate those issues to executives in understandable terms.

Note that the CIP senior manager definition requires that your selection be given both "authority and responsibility" for the CIP program. Too many times I've seen the CIP senior manager given the responsibility, but too little authority to take action. This is like telling your CIP senior manager, "You're responsible for driving the CIP bus, but you don't get a steering wheel."

Support your CIP senior manager

Once you have selected a CIP senior manager, it is important to establish regular communications, possibly via weekly or biweekly briefings. Expect regular updates on compliance and security status, changes to the standards and regulatory environment, emerging threats, staff training and accomplishments, and other topics as needed.

In addition to open channels of communication, you need to provide the CIP senior manager with an adequate budget, staffing, and other business needs.

These actions help set the "tone at the top" that is so necessary to implement effective compliance and security programs in your organization.

You may want to consider treating your compliance program in a manner similar to your safety program, where compliance is given constant consideration, such as "tailgate briefings" before any compliance-related work is performed. I'm in no way saying that your safety program should take a back seat to anything, but only that similar techniques may also produce positive results in the compliance program.

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 Resource 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.

Enforcement Explained

By: Bridget Sciscento, Associate Counsel, Enforcement

Protecting the grid in normal and abnormal conditions using the Generation Protection Standards

For RF's Enforcement department, our primary responsibility is reviewing and processing all identified instances of noncompliance. We invest time and resources in identifying patterns and trends in those noncompliances and while not all patterns have a discernable meaning or clearly attributable causes, the purpose of identifying trends is to pinpoint areas of potential increased risk.

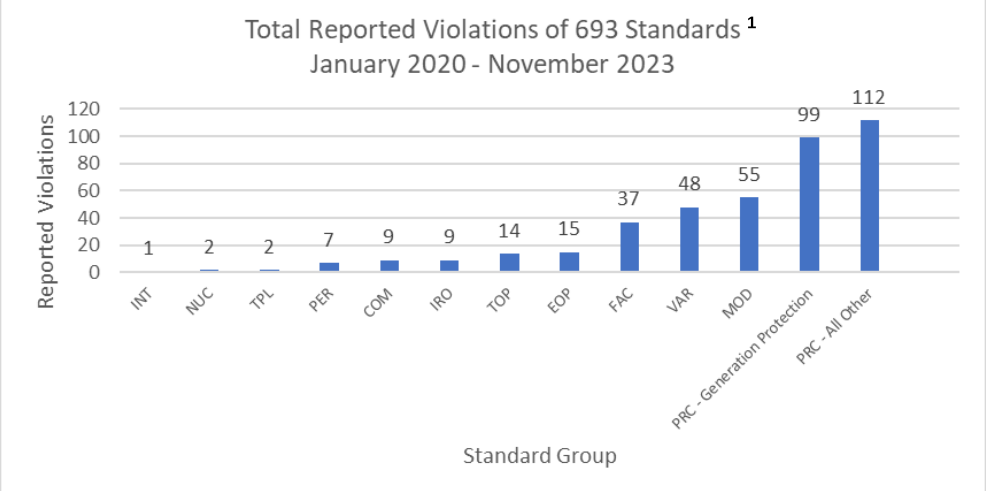
One trend that's stood out recently in this analysis involves the NERC Reliability Standards governing Generation Protection, specifically PRC-019, PRC-024, and PRC-025. From January 2020 through November 2023, the PRC standard group had the most reported instances of noncompliance among NERC Operations and Planning Standards by a large margin (156 more reported violations than the second highest, the MOD standard group). Within the PRC standard group, RF has noticed a marked increase in violations of PRC-019, PRC-024, and PRC-025 (the Generation Protection Standards), which make up approximately 47% of reported violations of the PRC Standard Group as a whole (see chart to the right).

These three PRC standards are interrelated and overlap in their purposes. PRC-019 focuses on coordinating generator unit equipment capabilities, voltage controls, and Protection Systems. PRC-024 and PRC-025 protect against unnecessary tripping during BES disturbances. Specifically, PRC-024 addresses frequency and voltage protection settings for generating resources, and PRC-025 governs the loadability of generator relays. In short, these Generation Protection Standards are designed to ensure relays will not unnecessarily trip under normal system conditions and to prevent the unnecessary and unexpected loss of more generation than necessary during extreme conditions.

These standards demonstrate their value and purpose at the most important time: when the grid is in a vulnerable state. They are standards that help industry to prevent and control system events during severe weather events, like Winter Storm Elliott, as well as amidst the ongoing changing generation mix, including the retirement and replacement of generators. When entities ensure that they are meeting the requirements of, and prioritizing, the Generation Protection Standards, they are not only complying with regulatory standards but protecting their equipment from potential damage and their customers from power losses when they may be most vulnerable.

Underlying noncompliance data and volume

From January 2020 through November 2023, RF received 99 violations (an average of approximately 25 per year) of the Generation Protection Standards. This represents an increase from already high numbers in 2018 and 2019 when RF received 43 violations (an average of approximately 21 per year) of the Generation Protection Standards. While an increase in violations does not equate to an inherent elevation of risk, it does indicate that resources may need to be allocated to ensure these Operations and Planning Standards are not becoming a footnote in compliance programs.



Common underlying root causes leading to violations and how to proactively work toward compliance

In reviewing the underlying cases, RF has recognized three common root causes: (1) lack of timely planning; (2) lack of sufficient knowledge and understanding of requirements; and (3) lack of adequate contractor oversight and internal control measures.

First, many of the Generation Protection Standards have time-based triggers which require entities to identify upcoming needs for modeling, testing, and other activities well in advance of the compliance deadline. RF has noted a common trend in root cause is an entity's failure to adequately plan ahead and provide themselves with sufficient buffer to accommodate

Continued on page 20

Enforcement Explained

Continued from page 21

unexpected setbacks (e.g., cancellation of planned outages, weather events preventing testing). To ensure that deadlines are not passing without the necessary requirements being performed, entities need to start looking at how they are going to comply with, for example, a five-year requirement in the years, not days or months, before the deadline.

Second, some of the Generation Protection Standards included phased-in implementation over a multi-year period.[2] NERC and FERC provide entities with runways to develop and institute compliance programs, but nevertheless, we are seeing entities that misunderstand specific requirements and expectations, and entities that misunderstand, or take incorrect approaches to, phased-in implementation.

For example, in an instance of PRC-019 noncompliance, an entity failed to understand that the coordination described in Requirement 1 needed to be verified following an equipment upgrade that could affect coordination. In other instances of noncompliance with these standards, entities failed to understand that certain types of relays were subject to the requirements. When a standard becomes effective, adequate training for relevant staff is key to successful and timely compliance.

The staff responsible for executing the requirements and sub-requirements of any given standard should be trained on their specific responsibilities within the standard's compliance landscape. Entities need to be proactive about identifying their applicable assets and determining where each asset fits into implementation milestones to avoid missing milestone deadlines.

Third, RF notes that numerous violations of the Generation Protection Standards arose from a lack of adequate internal controls to verify either the entity's own work or the work of third-party contractors. When entities contract with third parties to perform studies, installations, and other activities, entities should have procedures in place to verify that work in real or near-to-real time. RF recognizes that the Generation Protection Standards apply to entities of many sizes, which can make certain levels of verification resource-prohibitive. However, simple mechanisms such as checklists confirming certain key metrics prior to powering on a generator after service or a study may aid in identifying (and thereafter correcting) an issue.

Concluding Thoughts

At RF, the volume of violations of the Generation Protection Standards is of concern because these standards represent the guardrails that support the grid when conditions are normal and protect the grid when conditions become abnormal. As the generation mix changes and severe weather events become more common, the frequency of abnormal grid conditions may increase, and it's critical that steps are taken ahead of time to ensure that reliability is sustainable during abnormal conditions.

[1]There were no violations of the BAL Standard Group reported to RF between January 2020 and November 2023.

[2]The effective dates for the Analyzed PRC Standards are as follows. Please note that many of these standards had phased implementation plans meaning that each standard did not apply to all entities or all entity assets on the effective date.

PRC-019-2	July 1, 2016	Phased Implementation per PRC-019-1 Implementation Plan
PRC-024-2/3	Version 2: May 29, 2015; Version 3: Oct. 1, 2022	No phased implementation for Version 3
PRC-025-2	July 1, 2018	Phased implementation

Contact Entity Engagement

We encourage registered entities to reach out to our Entity Engagement team if they have questions regarding their approach to the issues discussed in this article.

FERC, NERC, and Regional Entities issue Winter Storm Elliott joint inquiry report

On Nov. 7, FERC, NERC, and the Regional Entities issued the final joint inquiry report on Winter Storm Elliott, the winter 2022 storm that contributed to power outages for millions of electricity customers in the Eastern U.S. FERC Chair Willie Phillips issued the following statement with the release of the report: "The FERC and NERC teams analyzed what happened, what went wrong, and the steps utilities, grid operators and stakeholders must take to avoid this in the future. I want everyone to take time…to read this report and begin implementing these recommendations, particularly those addressing the interdependence of gas and electricity. The report highlights what I've called for before: Someone must have authority to establish and enforce gas reliability standards."

Highlights from the report include the following:

- There were 1,702 individual BES generating units that experienced 3,565 outages, derates, or failures to start: 47% natural gas, 21% wind, 12% coal, 3% solar, 0.4% nuclear, and 17% other (oil, hydroelectric and biomass). These were caused by a mix of freezing issues, fuel issues, and mechanical/electric issues (which correlated to cold temperatures).
- At the worst point in the event, there were 90,500 MW of unplanned outages, derates and failures to start. In total, there was over 5,400 MW of firm load shed during the event.
- The Marcellus and Utica shale production dropped 23-54% during the event, due to wellhead freeze-offs, other natural gas supply chain equipment freezing, and weather-related poor road conditions that prevented necessary maintenance.
- The event is the fifth in the past 11 years in which unplanned cold weather-related generation outages jeopardized BPS reliability.

The report recommends the completion of the remaining cold weather Reliability Standard revisions identified after 2021's Winter Storm Uri, and for robust monitoring of compliance with the existing cold weather Reliability Standards. The report also has several winterization recommendations for generator owners and operators, and recommends an independent technical review of the causes of cold-related mechanical and electrical generation outages to identify preventive measures.

The report states that congressional and state legislation or regulation is needed to establish reliability rules for natural gas infrastructure to ensure cold weather reliability. It also recommends for the North American Energy Standards Board to convene a meeting of gas and electric grid operators and gas distribution companies to identify any needed communications improvements, and for an independent research group to analyze whether additional gas infrastructure is needed to support grid reliability.

FERC issues Order 901 on Inverter Based Resources (IBRs)

On Oct. 19, FERC issued an order (Order 901) directing the development of Reliability Standards related to inverter-based resources (IBR), such as wind, solar, fuel cell, and battery storage. The Reliability Standards will address four specific areas:

1. Data sharing: generator owners, transmission owners, and distribution providers need to share validated modeling, planning, operations, and disturbance monitoring data for all IBRs with planning coordinators, transmission planners, reliability coordinators, transmission operators, and balancing authorities.

2. Model validation: all IBR models need to be comprehensive, validated, and updated in a timely manner.

3. Planning and operational studies: planning and operational studies need to include validated IBR models to assess reliability impacts of IBRs. The studies also need to assess the impacts of IBRs within and across planning and operational boundaries for normal operations and contingency event conditions.

4. IBR Performance Requirements: IBRs need to provide frequency and voltage support during frequency and voltage excursions, and there needs to be clear and reliable technical limits and capabilities for IBRs to ensure they are operated in a predictable and reliable manner. IBRs need to contribute toward meeting the overall system needs for essential reliability services, and there needs to be post-disturbance ramp rates and phase lock loop synchronization requirements in place for IBRs.

NERC will file the new or revised Reliability Standards in three specified groups (each addressing different areas) over the next three years. NERC will also submit an informational filing to FERC that includes a comprehensive standards development and implementation plan for these Reliability Standards.

House of Representatives Energy Subcommittee holds hearing on grid reliability

On Sept. 28, the House Energy, Climate, and Grid Security Subcommittee held a hearing titled “Powering America's Economy, Security, and our Way of Life: Examining the State of Grid Reliability.” The hearing focused on Regional Transmission Organizations (RTOs) and Independent System Operators (ISOs), and RTO/ISO executives provided testimony. The full hearing is available to watch here. Issues discussed during the hearing included:

- The current state of the RTO/ISO energy and capacity markets.
- The impact of federal and state environmental regulations on reliability.
- The impact of price signals and incentives on market formation and the impact on reliability.
- How RTOs and ISOs are adapting to the changing generation mix.
- The state of regional and interregional transmission planning and development across RTOs and ISOs.
- The state of coordination between the RTOs/ISOs and the interstate natural gas pipelines.

FERC holds technical conference on reliability

On Nov. 9, FERC held its annual Reliability Technical Conference. NERC CEO Jim Robb gave a “state of reliability” report, and discussed risks posed by the integration of inverter-based resources, extreme weather, and the changing resource mix. However, he reported that the rates of misoperations, human performance issues, and vegetation management issues are down, and that entities are doing a good job self-reporting and remediating issues. Mr. Robb also discussed efforts at NERC to speed up the Reliability Standards development process.

Key areas of discussion during the conference’s panel discussions included the changing resource mix/resource adequacy, cyber security and the CIP Standards, and the impacts of the EPA’s proposed “Clean Power Plan 2.0” on reliability. During the EPA discussion, senior EPA staff discussed the EPA’s notice of proposed rulemaking under section 111 of the Clean Air Act, and fielded questions from the commissioners and expert panelists on it. The conference is available to view in its entirety here.

FERC issues Annual Report on Enforcement

FERC’s Office of Enforcement (OE) issued its seventeenth Annual Report on Enforcement. The report discusses the OE’s activities over the past year, including summaries of public audit findings and settlements, and anonymized discussion of nonpublic activities such as investigations, self-reports, and inquiries that were closed without further action. The report also provides a summary of the OE’s work on the joint reliability inquiry and report on Winter Storm Elliott.

The OE listed its top priorities in the report, which are fraud and market manipulation; serious violations of the Reliability Standards; anticompetitive conduct; threats to the nation’s energy infrastructure and associated impacts on the environment and surrounding communities; and conduct that threatens the transparency of regulated markets.

RF CIPC Meeting
Jan. 16-17, 2024

The RF Critical Infrastructure Protection Committee (CIPC) will be holding its first quarterly meeting of 2024 at the RF offices on Jan. 16 – 17. The purpose of the RF CIPC is to promote the physical and cyber security of critical electricity infrastructure in accordance with the NERC Critical Infrastructure Protection (CIP) Standards within the RF footprint.

The RF CIPC provides an industry-led forum for discussion and input among RF CIPC representatives responsible for physical and cyber security, including supply chain management. Any registered entity in the RF footprint can designate employees as CIPC representatives.

To prepare for this meeting, please ensure your list of RF CIPC Representatives is up to date. To obtain the list of your representatives or to make changes please email Lew Folkerth at lew.folkerth@rfirst.org or Nicholas Morton at namorton@aep.com.

To RSVP, click here.

Save the date...

2024 Fall Reliability and Security Summit
Sept. 17-18, 2024

Formerly known as the Fall Workshop, the 2024 Fall Reliability and Security Summit will take place Sept. 17-18, 2024, in Indianapolis.

Please save the date, mark your calendars, and stay tuned for additional information on topics and agendas.

If you or your company would like to be considered as a presenter at our event, please fill out the form located on our website.

2024 Protection and Human Performance Workshops
Aug. 7-8, 2024

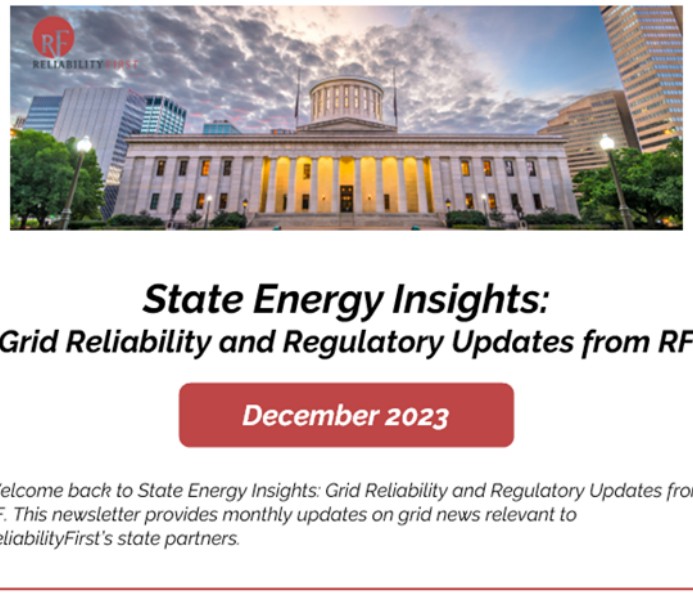
The 2024 Protection System and Human Performance Workshops are tentatively planned for Aug. 7-8 in-person at the RF offices in Independence, Ohio. Stay tuned for more details as we get closer to the event date next year.

ReliabilityFirst launches new website

Have you seen the new RFirst.org? We launched our new website in November! Come explore our new and improved look and feel, with a menu layout streamlined for the needs of entities, states and communities. Other highlights include a new searchable Resource Center, with filters by topic, year, and more. Check us out at RFirst.org!

Get grid updates tailored for state-level decision makers

Have you seen our State Energy Policy Newsletter? Click here if you'd like to subscribe to get monthly updates on grid news relevant to RF's state-level stakeholders. RF is an objective technical resource states can call on as they navigate difficult decisions related to the changing nature of the generation mix, extreme weather and more.



Outreach recap

RF is committed to providing timely and pertinent information to our entities and stakeholders. Our monthly, open webinars provide a forum to address topics and questions relevant to reliability, resilience, and security. During our Technical Talks with RF, we host a range of speakers and subject matter experts across the industry.

The Technical Talks with RF are typically the third Monday of each month (but may be moved to accommodate our speakers or to avoid holidays). Our calendar of upcoming events, with agendas and the Webex link to join, can be found on our website rfirst.org.

Some of the speakers this quarter have included the following:

October

Cybersecurity, Energy Security, and Emergency Response (CESER) and Idaho National Laboratory (INL) Cybersecurity Training for the Utility Workforce

Cynthia Hsu – Cybersecurity Program Manager, Rural and Municipal Utilities, Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response (CESER)

- Cynthia Hsu provided an update on upcoming cybersecurity training events hosted by CESER and INL. The training is designed for technical practitioners in electric utilities that require a hybrid of skills across information technology (IT), industrial control systems (ICS), operation technology (OT), cybersecurity, and electric grid operations.

BES Cyber Security (BCS) in the Cloud

Tom Alrich – Independent Consultant, Blogger and Leader of Open Web Application Security Project (OWASP), Software Bill of Materials (SBOM) Forum project

- Tom Alrich shared his thoughts regarding cyber security and CIP compliance in cloud environments. He discussed opportunities, risks and mitigations as industry explores the possibility of implementing BES Cyber Systems (BCS) into the cloud, including implications on CIP-002 and additional NERC Standards.

BES Cyber System Information Access Management

Shon Austin – Principal Technical Auditor, RF

- Shon Austin discussed Project 2019-02 BES Cyber System Information Access Management. This initiative enhances BES reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for entities to manage their BES Cyber System Information, by providing a secure path towards utilization of modern third-party data storage and analysis systems. In addition, the proposed project would clarify the protections expected when utilizing third-party solutions (e.g., cloud services).

November

NERC Interregional Transfer Capability Study, the aspects of the clean energy transition, and emerging technologies

John Moura – Director, Reliability Assessment and Performance Analysis – North American Electric Corporation (NERC)

- John Moura provided an overview and discussed the scope of NERC's Interregional Transfer Capability Study (ITCS). As directed by Congressional action, NERC is working on this study, in conjunction with the Regional Entities and industry stakeholders. The study focuses on the reliable transfer of electric power between neighboring transmission planning areas.

Shane Watts – Sr. Lead Trainer – PJM Interconnection

- Shane Watts discussed various emerging technologies and tools being developed and used to maintain reliable operation of the electric system. In addition, he highlighted Renewable Portfolio Standards (RPS) and goals within the PJM footprint.

December

EOP-011 and future EOP-012 on-site walkdowns

Beth Rettig – Senior Technical Auditor, RF

James Baird – Interim Plant Manager, Springdale Energy

Colleen Campbell – Director of Generation NERC Compliance, LS Power

Sandra Kennedy –NERC Compliance Manager, LS Power

- Beth Rettig introduced RF's perspective on EOP-011 and EOP-012 walkdowns.
- James Baird provided a high-level overview of Springdale Energy's EOP-011 winterization plan and EOP-012 preparation steps.
- Colleen Campbell and Sandra Kennedy reviewed LS Power's EOP-011 walk down experience and discussed lessons learned and offered a look-ahead at their organization's EOP-012 preparations.

ERO Enterprise 2024 CMEP Implementation Plan

Rashida Caraway – Manager, Risk Assessment, Texas RE

- The 2024 CMEP Implementation Plan describes the risks that will be priorities for the ERO Enterprise's CMEP activities in 2024. Rashida Caraway reviewed these risk priorities and how they factor into the overall reliability of the bulk power system.

Upcoming January 2024 Technical Talk with RF

Join us for our upcoming Technical Talk with RF on Monday, Jan. 22, 2024, from 2 - 3:30 p.m.

- RF Director of Enforcement Kristen Senk will review enforcement actions from 2023.
- In addition, Tim Fryfogle, RF Principal Engineer, Engineering and System Performance, will discuss both NERC and RF's latest Long Term Reliability Assessments.

Stay tuned for more details, including the Webex link, on our website calendar.

Calendar of Events

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

Date	RF Upcoming Events
Jan. 16, 2024	Critical Infrastructure Protection Committee Q1 Meeting
Jan. 22, 2024	Technical Talk with RF
Feb. 12, 2024	Technical Talk with RF
Feb. 23, 2024	Compliance User Group Winter Workshop
March 11, 2024	Technical Talk with RF

Industry Events

Date	Industry Upcoming Events
Jan. 18, 2024	FERC Open Meeting
Jan. 24, 2024	PJM Markets & Reliability Committee, PJM Member's Committee
Jan. 25, 2024	MISO Reliability Subcommittee
Feb. 14-15, 2024	NERC Board of Trustees meetings
Feb. 22, 2024	PJM Markets & Reliability Committee, PJM Member's Committee
Feb. 25-28, 2024	2024 NARUC Winter Policy Summit
Feb. 28, 2024	MISO Resource Adequacy Subcommittee
March 19-21, 2024	MISO Board of Directors meetings
March 20, 2024	PJM Markets & Reliability Committee, PJM Member's Committee
March 21, 2024	FERC Open Meeting


Happy Holidays from RF

ReliabilityFirst Members

AEP ENERGY PARTNERS
AES NORTH AMERICA GENERATION
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
INVENERGY, LLC
LANSING BOARD OF WATER AND LIGHT
MICHIGAN ELECTRIC TRANSMISSION CO, LLC
MICHIGAN PUBLIC POWER AGENCY
MIDCONTINENT INDEPENDENT SYSTEM OPERATOR, 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