PUBLIC

RELIABILITY FIRST

Issue 4 | 2022 Q4

Collaboration

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

Note from the President

Dear Stakeholders,

What a year it's been. We dove headfirst into state outreach in 2022, beginning in January with Jim Robb and I appearing before the Indiana state legislature and we never really slowed down. Throughout the year we talked to every state commission in our footprint and we are now more engaged with our states than ever before. Our efforts continued on other fronts as well. NERC issued a report developed by all the regions under SERC's leadership that outlines themes that lead to incorrect facility ratings. Our misoperation rate across the footprint continues to improve. And we helped NERC co-host this year's GridSecCon in October, just to name a few highlights from what was a non-stop 2022.

As we look to 2023, lots of challenges lie ahead. Decarbonization, decentralization and digitization will continue to be the number one topics of concern and in my mind, the biggest challenge in facing them is time. How do we achieve the results we all want to see without doing harm to reliability given the pace of the changes? As an Electric Reliability Organization (ERO), I think we have made a lot of inroads in spreading awareness and understanding of energy and capacity adequacy. In 2023 we need to move from this "tip of the spear" to all the other things that drive reliable electric supply – system restoration, short circuit duties, relays, dynamic stability and the capacity of the distribution system. Without them, adequate supply is useless and they cannot be an afterthought or worked on sequentially. Additionally, we must collectively work to continue to remove well-known, unnecessary risk from the table through maintaining accurate facility ratings, keeping misoperations low, preparing for extreme weather and practicing strong cyber hygiene, so we can be ready to deal with new, emerging, unknown risks coming our way in the future.

In the new year, I continue to urge you to participate in the NERC Standards Development Process. The standards process is facilitated by NERC and predicated on you as stakeholders actively working to propose new standards and to amend existing ones when risks to reliability indicate that is necessary. Entities have such tremendous power in the current standards development process and they must take advantage of it. Lately, there appears to be strong reliance on FERC ordering NERC to develop new standards or for a bad event to occur for us to determine if a new standard is needed for a new threat. I am hopeful the industry will be more proactive moving forward. Likewise, I encourage you to use your compliance efforts to become aware of risks that were hidden, have yet to emerge, were latent or unknown. When you are working with your internal subject matter experts, ask questions beyond the standards. Seek excellence. Whatever comes our way in 2023, we can be ready to tackle these challenges, but we must be proactive, diligent and work together.

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

Forward Together,

Tim

Issue 4 | 2022 Q4

INSIDE THIS ISSUE

Follow us on:

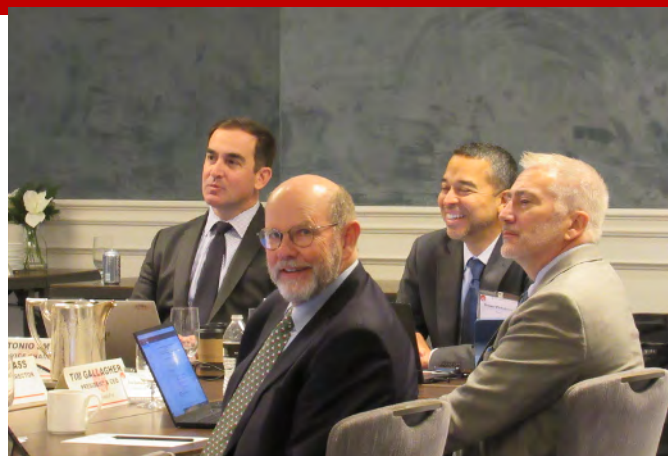
From the Board

RF held the 2022 Annual Meeting of Members on Dec. 8, 2022, in Arlington, Virginia.

Keynotes

FERC Director of the OER David Ortiz

The meeting began with a keynote from David Ortiz, FERC director of the Office of Electric Reliability (OER). Mr. Ortiz shared FERC focus areas and provided an overview of what the OER does, which includes implementing Section 215 of the Federal Power Act by: advising the commission on whether to approve standards, overseeing compliance, providing engineering support to rate filings and offices that manage commission work, monitoring the status of the Bulk Power System (BPS) and working with NERC's situational awareness team to review major events. Mr. Ortiz also discussed inverter-based resources and interconnection reforms as well as current priorities for the OER, which include:



From left to right: RF Board Vice Chair Antonio Smyth, NERC President and CEO Jim Robb, RF Board Chair Simon Whitelocke and RF President and CEO Tim Gallagher

- Maintaining a reliable and secure electric system with standards updated for the system we're moving toward, as the future of energy depends on it.
- FERC and NERC working together when they can, and when they can't, being complimentary, in order to provide effective reliability oversight.
- Ensuring cybersecurity coordination across the industry.

NERC President and CEO Jim Robb

NERC President and CEO Jim Robb also gave a keynote, highlighting challenges in the industry and walking through the history and changes from the 1965 blackout to today. Mr. Robb emphasized the need to find new ways to ensure resource adequacy with the growing demand and increased complexity of supply demand scenarios with the changing climate and expansion of Distributed Energy Resources.

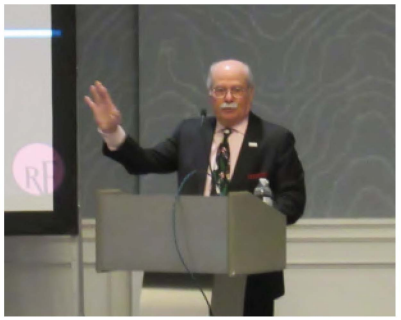
Mr. Robb noted the new and unfamiliar risks to the system and the increased complexity of conditions with climate change and the deeply electrified system, which will continue to increase the performance expectations of the industry. He shared the need for 21st century tools to manage an incredibly complex system of systems that will require a change planning mindset and a deeper understanding of fuel variability and new tools to manage inherent uncertainty to the grid. Mr. Robb also spoke to the rate of software vulnerability and said that as ransomware and organized criminals keep getting better, continued diligence is needed from everyone with system access. Mr. Robb underlined four priorities: energy, security, agility and institutional sustainability.

From the Board

RF President and CEO Tim Gallagher (left) and RF Board Chair Simon Whitelocke

Board notes

RF President and CEO Tim Gallagher gave the President's Report. He thanked Mr. Ortiz for being a steady hand and driving force leading the OER and Ken DeFontes, chair of the NERC Board of Directors and a founding member of RF, and Mr. Robb for being present. He welcomed Lesley Evancho and Scott Hipkins to the Board, noting they will fit in seamlessly and bring a wealth of knowledge and expertise. He also congratulated and welcomed back Jennifer Sterling, Ben Felton and Joe Trentacosta, following their reelection as members of the Board this year.



NERC Board of Directors Chair Ken DeFontes

Joanna Burkey, chair of the Nominating and Governance Committee, presided over the election of the at-large and independent directors, who will each serve three-year terms ending in December 2025. RF Vice President and General Counsel Niki Schaefer announced Mr. Trentacosta as at-large and Ms. Evancho as independent director.

Mr. Gallagher also shared some updates to his executive team, including welcoming Diane Holder as the Vice President of Entity Engagement and Corporate Services, highlighting the experience she brings from outside agencies. He also noted the recent promotion of Jeff Craigo to Senior Vice President of Reliability and Risk.

The Q4 Board of Directors Meeting followed the Annual Meeting of Members. Outgoing RF Board Chair Simon Whitelocke introduced Mr. DeFontes and recognized him as a pioneer of the RF Board. Mr. DeFontes recounted the beginning of the ERO and noted those who have helped build it along the way.

Brenton Greene

We say goodbye to Brenton Greene

A brief tribute to departing Lead Independent Director Brenton Greene was held, and remarks were shared from: former Board Chair Lou Oberski, former Board Chair Ken Capps, SERC CEO and former RF General Counsel Jason Blake and former RF Senior Vice President Ray Palmieri. Mr. Greene has been a part of RF since its inception and played a role in hiring Mr. Gallagher. Mr. Whitelocke emphasized that Brent's cybersecurity and national security expertise will be missed. Mr. Gallagher noted his long career in the service, his work in the intelligence community and the U.S. Navy and how he served as a member of various presidential commissions. Brent gratefully accepted the remarks and tokens of appreciation and shared that he was grateful for his time at RF and to have contributed to the ERO.

From left to right: RF President and CEO Tim Gallagher, departing RF Board Lead Independent Director Brenton Greene and RF Board Chair

From the Board

RF is pleased to introduce its 2023 Board of Directors. We welcome Antonio Smyth as our new chair, Nelson Peeler as our new vice chair, Patrick Cass as our new lead independent director, Scott Hipkins as a new transmission sector representative and Lesley Evancho as a new independent director. You can find more information on the Board of Directors on our website.

ANTONIO SMYTH
Chair
Supplier
AEP

NELSON PEELER
Vice Chair
Transmission
Duke Energy

PATRICK CASS
Lead Independent

JOANNA BURKEY
Independent

LESLEY EVANCHO
Independent

SCOTT ETNOYER
At Large
Talen Energy

BEN FELTON
Medium-LSE
DTE Energy

TIM GALLAGHER
Non-Voting Member
ReliabilityFirst

COURTNEY GEDULDIG
Independent

SCOTT HIPKINS
Transmission
FirstEnergy Corp.

JASON MARSHALL
Small-LSE
Wabash Valley

KEN SEILER
RTO
PJM

RACHAEL SNEAD
Supplier
Dominion Energy

JENNIFER STERLING
Large-LSE
Exelon

JOE TRENTACOSTA
At Large
SMECO

SIMON WHITELOCKE
At Large
ITC Holdings Corp.

The 2023 Q1 & Q2 RF Board of Directors and Committee Meetings will be held April 26-27, 2023, in Cleveland, Ohio.

Continuous Improvement

By Sam Ciccone, Principal Reliability Consultant

Checklists

The Journey to Security, Resiliency and Reliability

"The checklist is one of the most high-powered productivity tools ever discovered."

— Brian Tracy, motivational speaker and author

Now that we are in the holiday season, many children around the world are making gift lists for Santa, and supposedly he is checking them twice. Some of these lists are clear, but some take some interpretation. While checklists seem like a very simple concept, following a few best practices can ensure they provide the benefit you are hoping to achieve. This article will discuss the efficacy of checklists, best practices, collaboration and real-world Bulk Power System (BPS) examples to improve not only human performance, but also the reliability, resilience and security of the BPS.

Checklists: The good and the bad

As the BPS continues to evolve and become more complex, it is becoming increasingly important to develop checklists that maximize efficiency and reduce human error.

Checklists provide an overview of the tasks at hand and provide assurance that no steps are missed. It is not good enough to just remember the steps, so the checklist gives you peace of mind that you have accomplished the tasks safely and successfully. It helps drive reduction in human error and reduces distractions when performing tasks safely and reliably.

The checklist becomes troublesome when it is not specific enough to be consistently applied. This is especially perilous when it involves industries where lives are at stake, such as hospitals, aviation and nuclear power plants. They are also problematic when they include too many steps in the task, some of which are so obvious they should not be on the list. And complacency can be a problem when a checklist is used by personnel who are "too close" to the job tasks, which may contribute to the omission of important steps.

Collaboration

Collaboration is a consistent theme in continuous improvement (CI), and no CI effort can fully succeed without it. Per *The Checklist Manifesto,* the checklist is not developed by a single person or group in isolation, but by a group of stakeholders collaborating on the steps in the checklist and determining the detail needed in the checklist to deliver consistent results.

The group developing the checklist should collaborate to ensure each step is not thoughtlessly checked, allowing people to discover and act upon improvement opportunities. The checklist should also be tested to ensure any missing tasks are identified and added.

The cycle of continuous improvement remains intact when collaboration is part of your culture.

NERC Standards example checklists

Here are some examples of checklists and best practices:

Operations and Planning[1]

- Checklists for PRC-005 (Protection System, Automatic Reclosing, and Sudden Pressure Relaying Maintenance) Maintenance Activities for DC supply (batteries):
  - Checklists can be effectively used to demonstrate that some required maintenance activities have been performed per PRC-005.
  - Some maintenance activities cannot be demonstrated with a "check mark" – values will need to be recorded.

- Best practices for PRC-005 checklists:
  - Provide acceptable ranges associated with the check mark.
  - Use terminology in the checklist that is consistent with the terminology in the standard.
  - Use a checklist that is tailored for the specific component and not a generic checklist that might be applicable to multiple types of components.

Continued on page 7

Continuous Improvement

Continued from page 6

- Checklists for EOP – 008 (Loss of Control Center Functionality):
  - This is an example of a checklist that can be used for operational purposes.[2]
  - Ensure all systems/tools have been started and are operational at the backup Control Center.

- Best practices for EOP-008 checklists:
  - Make sure the checklist has all relevant/necessary items to ensure the proper operation of the backup Control Center.

Critical Infrastructure Protection[3]

- One common use of checklists in the CIP Standards is a commissioning checklist for new Cyber Assets. A successful checklist will include the steps needed to commission a new Cyber Asset, the order those steps must be performed in, and the compliance evidence to be gathered at each step.

- Best practices for new Cyber Assets checklists:
  - Ensure the checklist captures compliance evidence for each step. For example, a checkbox completion is not sufficient evidence that a vulnerability assessment for a new Cyber Asset has been performed as required by CIP-010-4 (Configuration Change Management and Vulnerability Assessments) R3 Part 3.3. The results of the vulnerability assessment should be documented and attached to the checklist.

Takeaways

There are right ways and wrong ways to develop and use checklists. Collaboration is important in all the work we do, especially when creating checklists. "Checklists are like any tool in our toolbox—they are helpful in some situations, but not a one-size-fits-all solution. Most important, checklists should increase both our self-awareness and our situational awareness. If they are shutting down conversation and creativity, it might be time to put a check on your use of checklists."[4]

I encourage all of you to read *The Checklist Manifesto*, one of the premier and most referenced books about checklists that exists.

To all our entities, thank you for reading our CI articles. I hope you all have a wonderful holiday season!

[1] The Checklist Manifesto, Atul Gawande

[2] Example provided, Glenn Kaht, Principal Reliability Consultant, Entity Engagement

[3] Example provided, Lew Folkerth, Principal Reliability Consultant, Entity Engagement

[4] Checklists Can Help Us Make Better Decisions - But Only When We Use Them Mindfully, Naz Beheshti Contributor

Checklist usage can prevent events

The NERC ERO Cause Code Assignment Process includes event cause codes related to the use of checklists.

Examples include:

- "*A5B1C03 – Checklist LTA,"* which discusses checklist confusion and lack of clarity, as well as;
- *"A4B3C11 – Inadequate work package preparation,"* which includes checklists that did not have adequate instructions for the work to be completed.

For more details, see the link to the process document above, or you can reach out to RF's Operational Analysis and Awareness (OAA) group via our website.

The Lighthouse

By Lew Folkerth, Principal Reliability Consultant

Finding and fixing trouble spots in your Incident Response Program

In the past few months, RF has observed multiple issues with incident response in both CIP-008-6 (Incident Reporting and Response Planning) and CIP-003-8 Attachment 1 Section 4 (Cyber Security Incident Response). In this article I'll discuss some of the finer points of incident response at both the high/medium and the low impact ratings. I'll designate which impact ratings are applicable with a [H/M/L] at the beginning of each section.

[H/M] Define attempts to compromise

CIP-008-6 R1 Part 1.2.1 requires you to include a definition of "attempts to compromise" in your Cyber Security Incident Response Plan (CSIRP). This definition should provide your incident response team (IRT) with a well-defined set of criteria to determine if an event is an attempt to compromise an applicable system. This should not be a judgment call, but rather a formal set of criteria that is clearly documented and that your IRT can implement during a suspected incident.

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.

[H/M/L] Scope of CSIRP

Each BES Cyber System (BCS) should be covered by one and only one CSIRP. You must be able to demonstrate to CMEP staff which CSIRP applies to a selected BCS. This is not usually an issue if you have only one CSIRP for all your applicable systems, but some entities have a separate CSIRP for field assets such as substations. In this case, there should be a bright line to determine the scope of the substation CSIRP. Does the substation CSIRP include the front-end processors that communicate with the substation RTUs? Or are the front-end processors part of the SCADA CSIRP? You're free to handle a circumstance like this as you choose, but your choice must be clearly documented.

[H/M] Interaction with CIP-007-6 R4 Part 4.1

CIP-007-4 R4 (Security Event Monitoring) requires you to log events for the identification of Cyber Security Incidents. During development and exercise of your CSIRP, you should review the logs available to the IRT. If additional logging is needed, you should address these needs in your CIP-007-6 R4 process.

[H/M/L] Ensure the CSIRP addresses operational needs

Some entities use a CSIRP developed for use by their entire organization. Such a comprehensive CSIRP is usually developed by the organization's Information Technology (IT) group. There is nothing inherently wrong with this. You should

Mainstique East Breakwater, MI – Photo: Lew Folkerth

Continued on page 9

Continued from page 8

ensure, however, that your CSIRP meets the needs of your Operational Technology (OT) assets. This will require close collaboration between your IT and OT security groups. For any OT incident response, you will need OT representation on the incident response team. As a case in point, I've seen CSIRPs that call for immediate network isolation and/or shutdown of a compromised asset. This may be an issue for a substation relay or a controller in an operating plant. Your CSIRP should address these types of systems in an appropriate manner.

[H/M/L] Use of OE-417 to report a Reportable Cyber Security Incident

If you are submitting an OE-417 to report an issue to the Department of Energy, there are boxes you can check to have the report forwarded to NERC, the E-ISAC, or CISA Central. This may be a valid method to perform the required reporting but be aware that you are still responsible for ensuring that E-ISAC and CISA Central have received the report, and that those organizations have received the report within the time required by the Standards. I recommend directly reporting any Reportable Cyber Security Incident to the E-ISAC and CISA Central. You should record the following for compliance purposes:

- Date and time the determination of a Reportable Cyber Security Incident was made
- A copy of the report sent to each required entity and the date and time the report was submitted
- A copy of the acknowledgement of receipt of each report

[H/M/L] Testing the CSIRP

When testing your CSIRP, be sure that you are testing using a Reportable Cyber Security Incident. Testing the plan using a physical incident or a Cyber Security Incident that is not reportable will not fulfill your compliance obligations in this area. You must choose a scenario that models a compromise or disruption of an applicable BES Cyber System, Electronic Security Perimeter or Electronic Access Control or Monitoring System.

If your CSIRP is part of a larger plan, ensure you test the part of the CSIRP that applies to your CIP systems.

Ensure you test each CSIRP for each Registered Entity. If you are using the same CSIRP for multiple Registered Entities, you must test the plan for each Registered Entity. If you have multiple CSIRPs for a single Registered Entity, you must test each CSIRP. As part of each test, you should ensure that the events logged as required by CIP-007-6 R4 Part 4.1 are sufficient to enable your incident response team to respond to an incident and to make a determination of a Reportable Cyber Security Incident.

RF provides the Incident Response Preparedness Assessment (IPRA) service to enable you to assess your preparedness for an incident. See the Resources section below for a link.

[H/M/L] Participate in development (2022-05)

NERC has established Project 2022-05 to draft revisions to CIP-008-6 to address "Modifications to CIP-008 Reporting Threshold." I recommend that you participate in, or at least monitor, this effort to strengthen the reporting threshold for Cyber Security Incidents. I included low impact as being affected by this because any change to the definitions will affect the low impact requirements as well.

[H/M/L] Resources

Incident Response Preparedness Assessment (IPRA) is an RF service to assist you in assessing your preparedness for an incident.

Cyber Planning for Response and Recovery Study (CYPRES) contains recommendations for incident response and recovery.

Computer Security Incident Handling Guide (NIST SP800-61r2) provides fundamental IT incident handling practices. This is the go-to guide for incident response in the IT community.

Locate training for OT incident handling using this Google search: ICS SCADA incident response training

Top 5 ICS Incident Response Tabletops and How to Run Them explains how to conduct a tabletop incident response exercise for OT assets.

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.

Internal Controls

By Courtney Fasca, Technical Auditor

Look back and look forward:

Our 2020-2021 review for your future focus

ReliabilityFirst (RF) reviewed compliance monitoring data for 2020 and 2021, including audit findings such as Potential Non-Compliances (PNCs), Areas of Concern (AoCs), Recommendations and Positive Observations, in addition to self-reports to identify compliance trends and areas for future focus and improvement. This analysis was split into two sections, one for the O&P Standards and another for the CIP Standards.

Most violations were self-reported rather than observed on engagements, a testament to each entity's commitment to a strong culture of compliance and integrity. The major themes of these violations and audit findings are described below. In addition to the usual positive elements of a good compliance program (e.g., mock audits, near-miss investigations, root cause analysis), a robust internal controls program – with preventative, detective and corrective controls – could help alleviate some of the issues identified in the themes.

O&P: Overall, the major observed O&P themes encompassed training, documentation, improved procedures and general Internal Controls program issues.

Training is a key component to any program and helps to ensure procedures and processes are performed as intended. Training should produce results in which staff understand their roles, responsibilities and expectations, helping maintain compliance across standards.

Documentation refers to the importance of consistent and thorough records. For example, for maintenance activities, when the storm hit, what equipment was repaired or replaced? Were these changes properly documented and were records updated as needed? To avoid discrepancies across records, ask if there is a central record repository. Is there an opportunity to institute peer-checks or third-party reviews? Do my completed MOD-025 forms include all data fields required by the standard? Consistent and thorough documentation is key to proving compliance and ensuring all critical information is recorded.

Improved Procedures. This theme calls for for specificity in and timely updates to procedures. Are there reminders for what needs to be updated when a Standard changes? What about when equipment, footprint, departments or staff changes? And rather than stating every possibility allowed in the Standard, ask "does this procedure state what we *actually* do?" Procedures should show the specific steps or tasks that should be taken to achieve specific goal(s), not just repeat the Standard without specifying which process the entity follows.

Internal Control Program Issues. This theme itself shows that entities are working to create and improve their own internal control programs and is a great sign of commitment to continued compliance. Establishing strong internal controls can help with a multitude of compliance requirements, such as meeting implementation dates, ensuring notifications are timely, ensuring responsibilities are properly mapped in mergers and acquisitions, ensuring clerical errors that could become big mistakes down the road are minimized, and ensuring any control or process doesn't hinge on one person.

Some entities went beyond expectations (doing more frequent checks, adding additional measurements, etc.) and implemented strong controls and best practices. These entities often have strong training programs, good controls and trackers, and in cases where there are issues, they perform thorough extent of condition reviews and place importance on continuous improvement efforts.

These themes are captured in engagements as Positive Observations – evidence of entities understanding the role of compliance, demonstrating a sustainability mindset and achieving compliance at a high level.

Continued on page 11

Internal Controls

Continued from page 10

CIP

Entities continue to improve at detecting and reporting issues, indicated by the sustained reduction of PNCs found in CIP Audits, Spot Checks and Self Certifications from 2020-2021. Overall, this indicates a general maturation and enhancement of CIP Compliance programs through automation in several functional areas such as:

- Identity and access management systems for onboarding, tracking and revoking access
- Security patch and vulnerability management programs
- Use of new generation Security Event Information Monitoring (SEIM) systems for logging, monitoring and alerting
- Integrated use of configuration management systems for tracking ports and services and system baselines

While automation provides a solid basis for internal controls, entities must also demonstrate and document clearly how automation functions and supports programs. When configured properly and securely, automated processes can prevent, detect and correct issues more efficiently. With continued focus on internal controls, the trend should also continue to show more limited audit findings.

The Bottom Line:

Entities are showing commitment to reliability in their self-reports and internal controls program efforts, but continuous improvement is a must. Designing and implementing a strong internal controls program can help to address these major themes, spread across many Standards, departments and processes.

Internal controls help every organization mitigate their own specific risks and there are always opportunities for improvement. We cannot be complacent – risks evolve and so must our controls. We also cannot show off an internal controls program like a fancy car – where it looks so shiny and new, so sleek and impressive – but when you look under the hood of the car, the engine is missing! An effective internal controls program goes deeper than the surface level.

Consider attending the 2023 Internal Controls Workshop hosted by RF in Independence, Ohio. We will build off the previous 2019 Internal Controls Workshop, with short lectures and collaborative group activities concentrating on FAC-008, CIP-005 and CIP-007 risks. The workshop will be technical and interactive, so SMEs (in addition to their PCCs) are highly encouraged to attend!

More information can be found on the Eventbrite page. We hope to see you there!

Enforcement Explained

By: Mike Hattery, Counsel

2022 Enforcement Trends

A focal point for RF Enforcement in 2022 has been transparency. With that in mind, this quarter's column discusses metrics intended to provide further visibility into ReliabilityFirst's enforcement work in 2022.

Before diving into the data and potential implications, it is important to discuss three important caveats. First, the data is a broad snapshot, and while informative, it can be difficult to draw specific conclusions. The second key caveat is that RF Enforcement's data sharing choices balance a couple of important priorities: transparency and security. That is, especially in the CIP space, we want to provide context but not highlight areas of weakness in open violations such that they can be leveraged. For this reason, beyond discussion of total inventory, the primary matters discussed below are most frequently violated standards, processed dispositions and mitigated dispositions. Third, the data provided is limited to the RF footprint and not the ERO Enterprise as a whole.

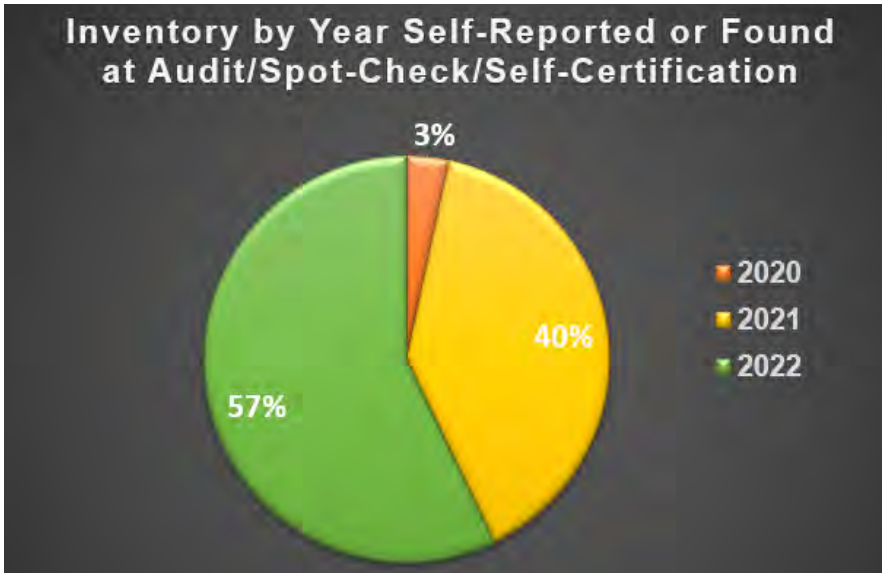
If you want further context about how your entity stacks up against industry-wide markers or what we are seeing as it relates to new violations, please reach out to your case manager.

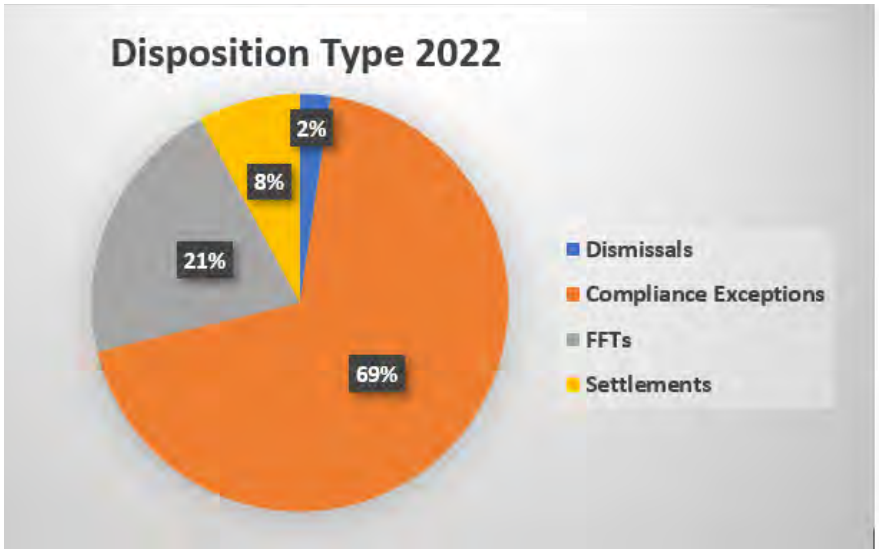
Open inventory leans current

Over the past three years, a central priority for RF Enforcement has been to clear out older inventory and slowly move open inventory more and more current. What you can see above is that in RF, 97% of the open noncompliances are from the past two years. Additional context on what is considered open inventory is important. These are noncompliances that have not been disposed of in a compliance exception, FFT, settlement or dismissal. In a majority of these cases, mitigation has been submitted, reviewed and approved. Therefore, while the disposition is not yet complete, the risk is being (and in a lot of cases, has been) mitigated.

2022 Disposition Type

One of the big takeaways, similar to data from prior years, is that 92% of the noncompliances disposed of in 2022 were done so outside of the penalty space. It is worth noting that for the five years prior, the number of noncompliances addressed outside of the penalty space was closer to 85%. However, that does not mean that the number of settlements is decreasing – it is not. Rather, the number of violations in settlements is decreasing (i.e., the settlements generally involve a narrower set of issues and violations).

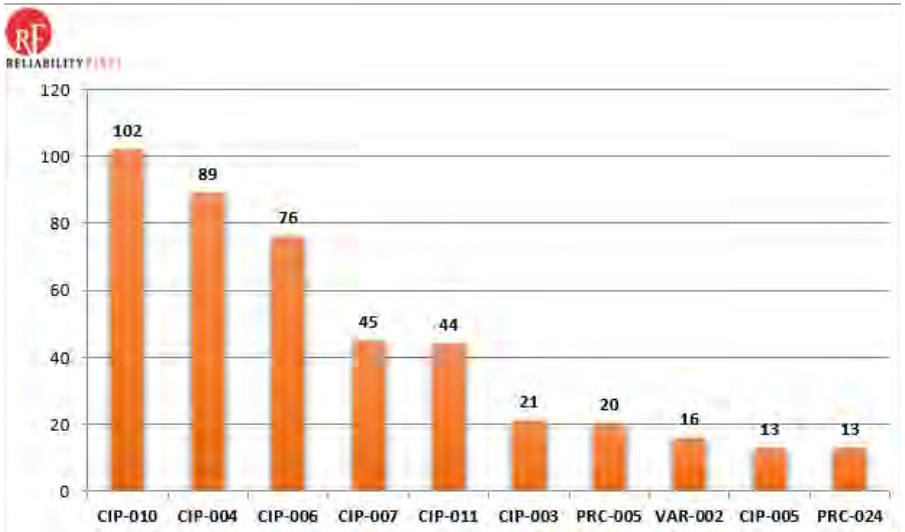




Continued on page 13

Enforcement Explained

Continued from page 12



The majority of violation intake remains CIP-centric

Since the start of 2016 and the implementation of CIP Version 5 standards, CIP noncompliances have generally constituted anywhere between 65-80% of ReliabilityFirst's inventory. One important caveat is that the volume of CIP noncompliances is not an indication that they are elevated in risk as compared to the operations and planning side. A significant component of the CIP volume arises from what are often referred to as the high-frequency conduct standards.

Three digestible examples of high-frequency conduct requirements are:

- CIP-010-3 R1.2/R1.3 (authorizing and documenting changes or deviations from the existing baseline)
- CIP-007-6 R2 (security patch management)
- CIP-004-6 R5 (access revocation)

Essentially, these are standards and requirements that require the successful completion of so many individual acts such that small individual variances from compliance can be expected.

As outlined above, a handful of the high-frequency conduct requirements rest in the top-5 most violated standards. There are also a couple of interesting observations based on the chart above. CIP-007 is the most violated standard in ReliabilityFirst's history. While it remained a frequently violated standard in 2022, its downshift is worth considering.

However, whether this is a trend related to improving entity controls around patching and other CIP-007 activities or a statistical outlier is not clear as of this writing. Second, as has been true historically, PRC-005 and VAR-002 remained the two most frequently violated operations and planning standards.

Reach out to your case manager

What was detailed above is merely the tip of the iceberg when it comes to context and information your case manager can provide about how your entity compares. If you want more context or want to discuss particular issues that your entity is considering or facing, please reach out to your case manager.

Reliability Resource Risk Assessment

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

1. Capacity and Reserves - review of additional capacity resources (Planning Reserve Margin) compared to the Reserve Margin Requirement (resources needed to meet a loss of load expectation [LOLE] of one day in 10 years)
2. Random Generator Outage Risk Analysis - review of potential 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 MISO, PJM and RF assessments.

For the upcoming winter of 2022-2023, both MISO and PJM are expected to have adequate resources to satisfy their respective Reserve Margin Requirements. However, if the upcoming winter of 2022-2023 experiences higher than anticipated resource outages, there is a likelihood that the MISO area will need to utilize measures to serve forecasted load demand. Note that this risk increases in probability when the forecasted load demand for the 2022-2023 winter is higher than expected. These measures include Load Modifying Resources (or LMRs, MISO's demand response), non-firm transfers into the system, energy only interconnection service resources not receiving capacity credit, or internal transfers that exceed the Sub-Regional Import/Export Constraint (SRIC/SREC) between the MISO North/Central and South regions. The resource outage risk assessment is outlined below. It 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.

Reliable operation of the thermal generating fleet is critical to winter reliability and assured fuel supplies is an ongoing winter reliability concern. Present domestic and global affairs warrant even greater attention on generator fuel supplies, including natural gas, fuel oil and coal, for the upcoming winter. Inventories of coal and fuel oil in most areas are lower than typical following a summer of high electricity demand and high natural gas prices that made other fuels more economically advantageous for electricity generation. Low fuel storage levels coupled with a range of potential supply chain issues like fuel resupply challenges are creating additional risks for winter regional Bulk Power System (BPS) reliability. Careful attention to periodic fuel surveys is needed to provide early indication of fuel supply risks.

PJM Capacity and Reserves

Net capacity Resources [1]	184,376 MW
Projected Peak Reserves	57,979 MW
Net Internal Demand (NID)	126,397 MW
Planning Reserve Margin	45.9%

The PJM forecast Planning Reserve Margin of 45.9% is greater than the 14.9% Reserve Margin Requirement for the 2022 planning year. The Planning Reserve Margin for this winter is higher than the 2021 forecast level of 42%. This is due to an increase in existing certain generation and the decrease of sales of capacity to entities outside of PJM.

MISO Capacity and Reserves

Net Capacity Resources	141,565 MW
Projected Peak Reserves	42,626 MW
Net Internal Demand (NID)	98,939 MW
Planning Reserve Margin	146,296 MW

The MISO forecast Planning Reserve Margin of 43.1% is greater than their Reserve Margin Requirement of 17.9% for the 2022 planning year. The

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

Continued on page 15

Winter 2022-2023

Continued from page 14

Planning Reserve Margin for this winter is lower than the 2021 forecast level of 44.7%. This is mostly due to an increase in generation retirements in MISO's footprint and a decrease in capacity transfers into MISO.

RF Footprint Resources

Net Capacity Resources	194,470 MW
Projected Peak Reserves	58,388 MW
Net Internal Demand (NID)	136,082 MW
Total Internal Demand (TID)	143,809 MW

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 2022-2023 winter period.

Random Generator Outage Risk Analysis

The following analysis evaluates the risk associated with planned and random forced outages that may reduce the available capacity resources below the load demand obligations of PJM or MISO. Reports and/or other data released by PJM, MISO or NERC for this same period may differ from the data reported in this assessment due to different assumptions that were made by RF from the onset of the report. This analysis differs from NERC's in that RF uses actual historical GADS data from a rolling five year period which provides a range of outages that occur during the winter period.

The stacked bar charts in Exhibits 1 and 2 are based on forecasted winter 2022-2023 demand and capacity resource data for the PJM and MISO areas. 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 forced outages. The random forced outages are based on actual NERC GADS outage data from December, January and February of 2017 through 2021.

To assist the reader in better understanding Exhibits 1 and 2 on page 17, the following text is offered. The committed resources in PJM and MISO are represented by the Resources bar in shades of blue and only include the net interchange that is a capacity commitment to each market. Additional interchange transactions that may be available at the time of the peak are not included, as they are not firm commitments to satisfying each area'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 (NID), with Total Internal Demand including the effects of DR. The daily Operating Reserve requirement (shown in yellow) is between the NID and DR bars. There are two sets of stacked Demand bars on the chart, one representing the 50/50 demand forecast and one representing the 90/10 demand forecast. For instance, the 50/50 demand forecast projects a 50% likelihood that demand exceeds the forecast (e.g., 126,397 MW for PJM). The 90/10 demand forecast is a more conservative model, projecting a 10% chance that demand exceeds the forecast (e.g., 137,199 MW for PJM). Since DR is utilized first to reduce the load obligation when there is insufficient capacity, this part is at the top of the Demand bar. In the event that utilization of all DR is not sufficient to balance capacity with load obligations, system operators may first reduce operating reserves prior to interrupting firm load customers.

Between the Resources bar and the Demand bars is the projected Resource Outage bar. While scheduled outages during the winter season are generally minimal, there are a small number of outages that extend during the winter, which are reflected in the Scheduled Maintenance (colored gray) in the Outage bar. The remainder of the Outage bar represents the entire range of random forced outages. Pink shows 100% of the random forced outages, while rose

Continued on page 16

Winter 2022-2023

Continued from page 15

shows less than 100% down to 10% of the random forced outages. Additionally red shows less than 10% down to 0.2% of the random forced outages on the chart. All of the above occurred during the five-year reference period.

In the following discussion of the random forced outages, the analysis of random forced outages exceeding certain reserve margin targets is presented as a possibility.

These 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 winter periods that would have exceeded the reserve margin that is listed. They are discussed as probabilities as a matter of convenience in describing the analysis results.

To the left side of the range of random forced outages are probability percentages related to the amount of random forced outages that equal or exceed the amount of outages shown above that line on the Outage bar. Moving from top to bottom of the Outage bar represents an increasing amount of random forced outages, with a decreasing probability for the amount of random forced outages. In the PJM chart, the random forced outages represented by the bar above the 100% point is 537 MW.

This means that the probability of there being at least 537 MW of random generation outages is 100%. Similarly, at the 10% point, the outages represented by the bar above the 10% point is 20,546 MW (537 MW + 20,009 MW). There is a 10% probability that there will be at least 20,546 MW of outages. As shown by the probabilities and corresponding amounts of random forced outages, the distribution of random forced outages is not linear throughout the range of outages observed.

To the right of the Outage bar are the probabilities of the random generation outages that correspond to different levels of demand obligation. In Exhibit 1 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.

Exhibit 2 contains the information to perform the same analysis for MISO. The top of the 50/50 demand obligation with the operating reserves has a 1% probability that Demand Response will be required during normal demand.The top of the 90/10 demand obligation with the operating reserves has a 11% probability that Demand Response will be required during high demand.

Exhibit 1 - 2022/2023 Winter PJM Resources Availability Risk Chart

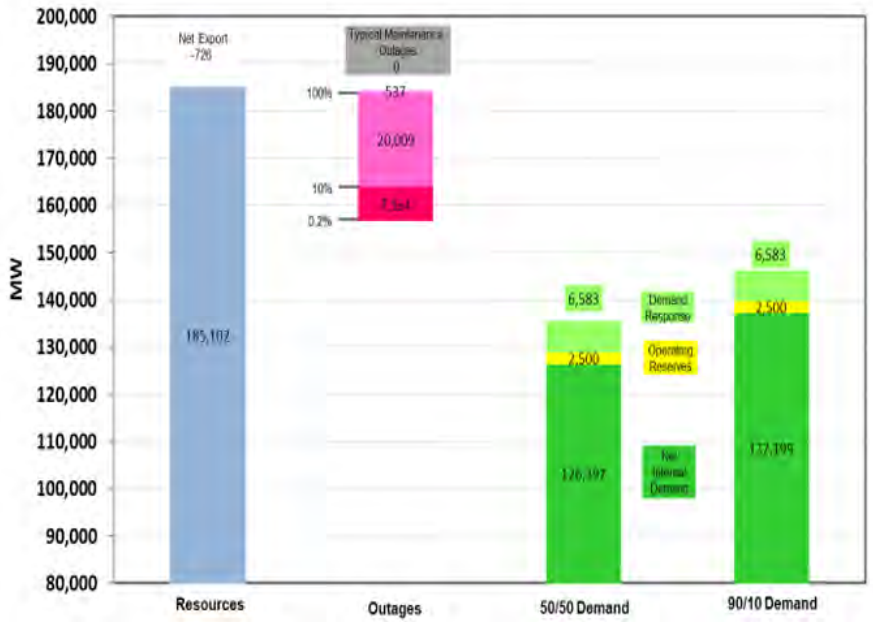
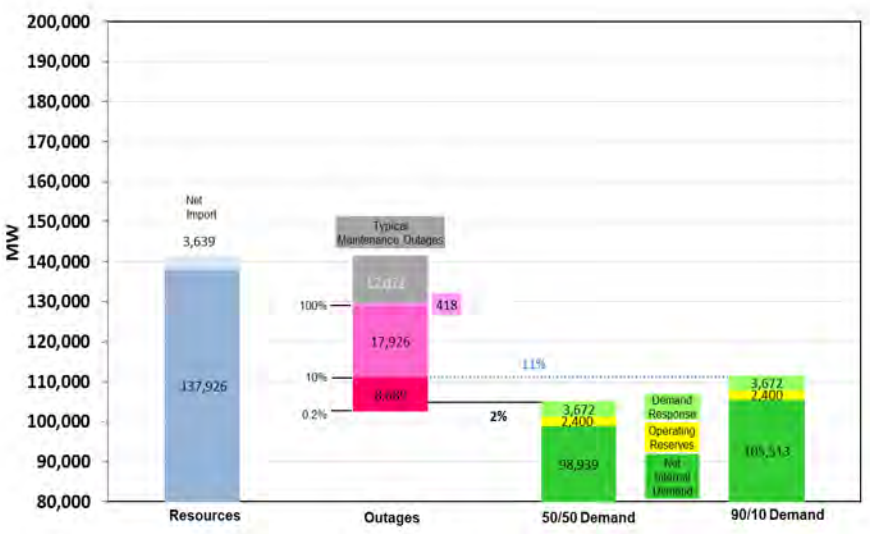


Exhibit 2 - 2022/2023 Winter MISO Resources Availability Risk Chart



2022 Long Term Resource Assessment for the ReliabilityFirst Region

ReliabilityFirst (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 amount 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.

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 the required milestones
>
> **Tier 2**: Includes capacity that has been requested 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 or 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.

Key Findings

- PJM is projected to have a 0.37% load growth rate over the next ten 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 0.30% load growth rate for 2023 through 2032.
- The MISO target reserve margin, which includes both Existing-Certain and Tier 1 resources, is projected to not satisfy its reserve margin target for the entire 10-year period. The largest reserve margin deficit was identified in 2032, which was 23,454 MW below the target reserve margin. Since these projected reserve deficits start next year, it is probable that up to 29% of Tier 2 and Tier 3 resources presently in the MISO generation queue will be needed for MISO to meet their target reserve margin requirement in 2032.
- The projected five-year out Anticipated Reserve Margins for MISO indicate a regional generation shift. In the event that all potential retirements occur without new replacement capacity, a shortfall below the Reference Margin Level in 2023 and beyond is projected to occur. Also, the extreme weather events of the past several years continue to stress the importance of ensuring the MISO Resource Adequacy construct sends the appropriate planning and operating signals that ensure members continue to perform reliably.

PJM

Capacity and Reserve Margin

PJM resources are projected to be 213,353 MW in 2023 and increase to 259,588 MW by the end of 2032. 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.

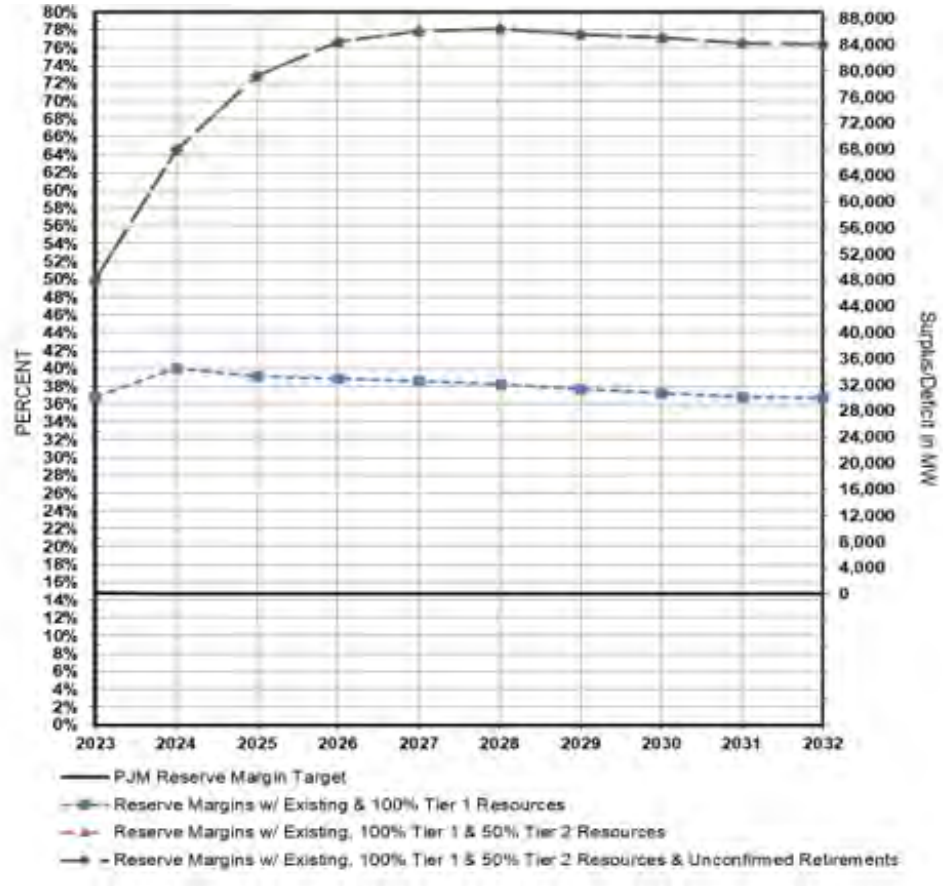
The figure to the left on page 19 shows the reserve margin for PJM from 2023 through 2032. Please note that varying resource scenarios are used to gauge how much of the generation queue (i.e., generation that is yet to be built) is needed to stay above the target reserve margin. The blue line represents PJM's reserve margin with both Existing-Certain and all Tier 1 resources. On average, PJM has a 38% reserve margin and is expected to meet and significantly exceed its target reserve margin (of approximately 15%) from 2023 through 2032.

Continued on page 18

2022 Long Term Resource Assessment for the ReliabilityFirst Region

Continued from page 17

PJM
Summer Reserve Margin Projections
2023 - 2032



Peak Demand

The figure to the right displays actual demand data with a ten-year forecast of demand for PJM. PJM's 10-year forecasted growth indicates that peak demand has flattened out over time. Based on the latest 2022 forecast, PJM is projected to average a 0.37% load growth per year over the next ten years. The PJM summer peak demand in 2023 is projected to be 149,351 MW and increase to 154,381 MW in 2032 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.

PJM RTO Peak Demand Data
Actual 2006 - 2021
Select 10 Year TID Forecasts Through 2032

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 19

2022 Long Term Resource Assessment for the Reliability Region

Continued from page 18

MISO

Capacity and Reserve Margin

MISO resources are projected to be 142,658 MW in 2023 and then increase to 210,018 MW by the end of 2032. This resource calculation includes planned generation retirements, planned generation additions and changes, and Tier 2 and Tier 3 projects from the generation interconnection queue.

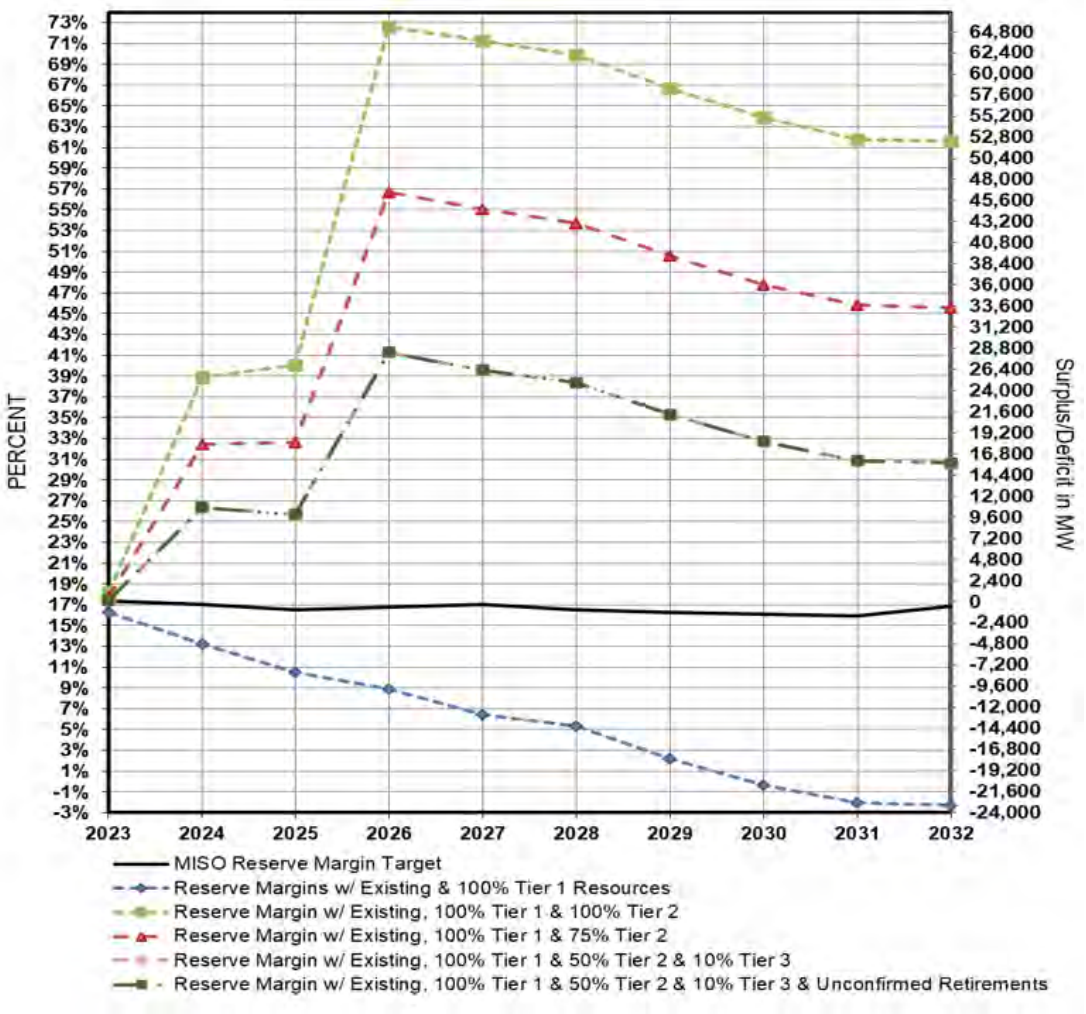
Since last year, 5,900 MW of generation has retired (mostly coal-fired generators) and 1,700 MW of new generation has been added (approximately 700 MW natural gas-fired, 400 MW Solar, 100 MW wind and 300 MW pumped storage). In summer 2023, MISO's capacity shortfall is projected to be 1,319 MW even after adding over 6.5 GW of new generation with signed interconnection agreements. More additions from the planning queue are not likely to be completed in sufficient quantity to make up for the capacity shortfall.

To be proactive, MISO conservatively solicits voluntary responses to assess potential resource outcomes via the Organization of MISO States (OMS)-MISO Survey process. This approach allows MISO and its members to discuss potential future resource deficiencies well in advance.

The MISO generator interconnection queue continues to show steadily increasing levels of variable energy resources including battery storage and hybrid resources in the future generation fleet mix. Currently 300 MW of grid-connected batteries are installed, with another 15 GW in the interconnection planning queue and 16 GW of hybrid battery-renewable generation in queue. This transition of the generation fleet, along with the observed extreme weather events of Hurricane Laura in 2020 and Winter Storm Uri in February 2021 continue to stress the importance of the MISO Resource Adequacy construct. Appropriate planning and operating signals must be sent to prompt investment (or system enhancements) when needed to ensure that the Bulk Power System (BPS) continues to perform reliably.

The figure on the previous page shows the reserve margin for

MISO RTO
Summer Reserve Margin Projections
2023 - 2032



Continued on page 20

2022 Long Term Resource Assessment for the ReliabilityFirst Region

Continued from page 19

MISO from 2023 through 2032. 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. MISO's anticipated reserve margin, which includes Existing-Certain and all Tier 1 resources, does not satisfy the target for 2023.

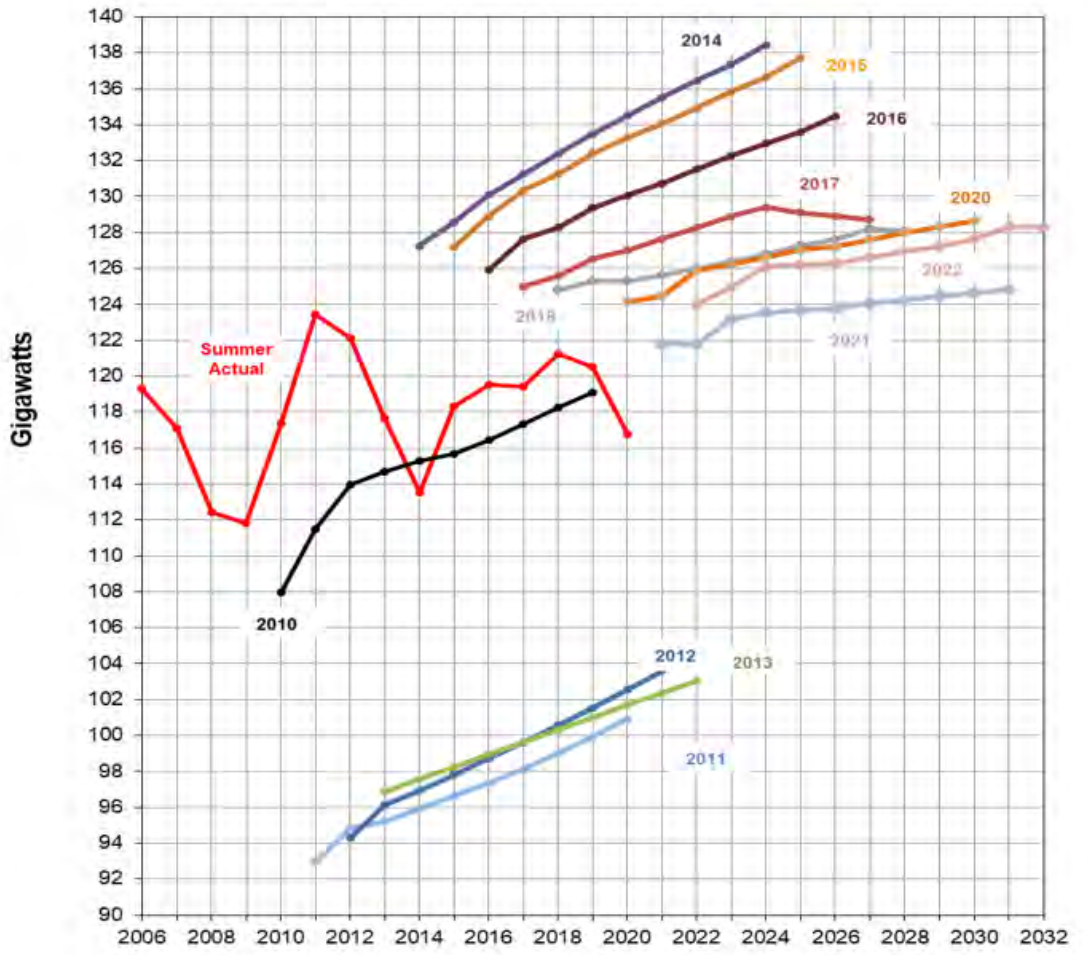
The MISO anticipated reserve margin projected for 2023 is 1,319 MW below the reserve margin target. Continuing in 2024, the projected reserve margin is 4,526 MW below the target and continues to decline to 23,454 MW below the target in 2032. These values are represented in the figure on the previous page with the blue line.

Peak Demand

The figure to the right displays actual demand data with a ten-year forecast of demand for MISO. MISO's 10-year forecasted growth indicates that peak demand has flattened out over time.

The projected MISO annual load growth rate for 2023 through 2032 is approximately 0.30%. The MISO summer peak demand is projected to be 124,950 MW in 2023 and 128,317 MW in 2032 for total internal demand (TID).

MISO RTO Peak Demand Data
Actual 2006 - 2021
Select 10 Year TID Forecasts Through 2032



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

New resource type supports energy transition

On Thursday, Sept. 1, MISO included Electric Storage Resources (ESRs) into its market portfolio for the first time. This new resource type has operational characteristics that support reliability and resilience as the industry continues to transition the resource fleet.

“We are excited to see this space grow with increasing member interest and participation, particularly as we continue to adapt to the accelerating resource transition,” said Jessica Lucas, MISO’s executive director – system operations. “With the introduction of Electric Storage Resources to our market portfolio, we will continue to position MISO’s grid and its members for the Grid of The Future.”

The Federal Energy Regulatory Commission (FERC) defines ESRs as “a resource capable of receiving electric energy from the grid and storing it for later injection of electricity back to the grid regardless of where the resource is located on the electrical system.”

Examples of ESRs include batteries, pumped storage facilities and compressed air energy storage. MISO’s ESR implementation enables the resources to participate in MISO’s Energy and Operating Reserves Markets as supply and demand.

“The MISO team has demonstrated excellent collaboration with our stakeholders, and the pursuit of creative solutions resulted in MISO’s first secured Patent,” Lucas continues. “The development of the ESR participation model has been a key element of the Market Redefinition pillar of MISO’s Response to the Reliability Imperative in the resource models and capabilities area.”

ESRs are flexible resources that can help reduce peak demands, manage congestion and provide backup power for major disruptions because they can respond quickly and switch between injection

(discharge) and withdrawal (charge) modes. The near-term benefits of the new ESR model are modest due to the small volume of storage resources. However, the new model positions MISO ahead of the increased storage participation anticipated with higher penetration of renewables and Distributed Energy Resources over the next five to 10 years.

FERC Issues Orders and Notice of Proposed Rulemaking on Inverter-Based Resources

On Nov. 17, FERC issued two orders and a Notice of Proposed Rulemaking (NOPR) related to regulation of inverter-based resources (IBRs), which include solar, wind, fuel cell and battery storage.

The first order directs NERC to develop a work plan within 90 days describing how it will identify and register owners and operators of IBRs that are connected to the BPS and "have an aggregate, material impact on the reliable operation of the BPS," but are not yet required to register under the Bulk Electric System (BES) definition. The work plan must address how NERC will include unregistered IBRs (*e.g.,*changing the BES definition, the registration program or another solution) within one year of its approval. NERC must identify entities meeting the new registration criteria within two years of the work plan's approval date and must register them and require them to comply with applicable Reliability Standards within three years of the work plan's approval.

The second order approves reliability standards FAC-001-4 and FAC-002-4, which NERC proposed earlier this year. FAC-001-3 required Transmission Owners and applicable Generator Owners to complete coordinated studies for new or "materially modified" existing interconnections. FAC-001-4 revises that requirement by applying it to "qualified changes" that can have reliability impacts instead of "materially modified" interconnections. Additionally, FAC-002-4 authorizes Planning Coordinators to define the term "qualified change" for their areas and requires that they publicly post their definitions. These modified standards will help ensure that changes to existing interconnected facilities that have reliability impacts are properly addressed in interconnection requirements and studies. This effort originated from recommendations in the NERC Inverter-Based Resource Performance Task Force's March 2020 white paper.

In the NOPR, FERC proposes to direct NERC to develop new or modified reliability standards addressing four reliability gaps related to IBRs: data sharing, model validation, planning and operational studies, and performance requirements. In the NOPR, FERC discusses reliability risks related to IBRs and notes that at least 12 events on the BPS have demonstrated common mode failures of IBRs acting adversely and unexpectedly. The NOPR then discusses the four identified reliability gaps to be addressed by the creation of new standards, and proposes to direct NERC to submit a standards development and implementation plan for new IBR-related reliability standards.

2022 FERC Staff Report on Lessons Learned from Commission-led CIP Reliability Audits

In October, FERC staff released its annual report that provides anonymized lessons learned from FERC-led non-public CIP audits of registered entities. The report states that entities audited met most of the CIP requirements, but there were some identified potential noncompliances and security risks. FERC also identified voluntary cyber security recommendations, which are practices not required by the CIP Standards, but which could enhance security.

The lessons learned from this year's report are in the following areas (additional detail can be found within the report):

1. CIP-003-8, R2: Re-evaluate policies, procedures and controls for Low-impact Cyber Systems and associated Cyber Assets.
2. CIP-007-6, R2.3 & CIP-010-4, R3.4: Address risks posed by BES Cyber Assets that have reached the manufacturer-determined end of life/service and are no longer supported by vendors.
3. CIP-007-6, R3: Deploy a comprehensive malicious code prevention program for all Cyber Assets within a BES Cyber System.
4. CIP-010-4, R3: Implement comprehensive vulnerability assessment processes for applicable Cyber Assets.
5. CIP-010-4, R4: Review and validate controls used to mitigate software vulnerabilities and malicious code on Transient Cyber Assets (TCAs) (portable electronic devices used for data transfer, vulnerability assessment, maintenance or troubleshooting purposes) managed by a third party.

FERC 2022 Report on Enforcement

In November, FERC staff issued its 2022 Report on Enforcement, which gives a summary of the FERC Office of Enforcement's activities (OE) over the past year. In the past year, OE has opened 21 new investigations and negotiated 11 settlements representing approximately $57.52 million in civil penalties and disgorgement. OE's 2022 priorities were fraud and market manipulation, serious violations of the reliability standards, anticompetitive conduct, threats to the nation's energy infrastructure, and conduct that threatens the transparency of regulated markets.

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 publishes strategic document on distributed energy resources

The Bulk Power System (BPS) is undergoing significant change and will continue to see substantive shifts over the coming decade. One of the key drivers is the specific benefits and challenges introduced by the influx of Distributed Energy Resources (DERs). In terms of reliability and resiliency, DERs present unique challenges on an increasingly large scale. In order to address these challenges, NERC rolled out a strategic document outlining, among other things, milestones for technical deliverables.

ERO Enterprise practice guide posted for modeling and studies involving DERs

On Oct. 13, 2022, the ERO Enterprise released a compliance monitoring and enforcement practice guide for modeling and studies involving DERs.

ERO Enterprise releases the Entity Onboarding Checklist

In order to provide additional information and context on the registration process, the ERO Enterprise has released the Entity Onboarding Checklist. The checklist outlines required activities for Registered Entity contacts and Registered Entities. Beyond required items, the checklist has recommended items as well.

NERC publishes Long-term Reliability Assessment

NERC released its 2022 Long-term Reliability Assessment on Dec. 15, 2022.

Notable FERC Orders

In October-November, FERC filed the following:

- On Nov. 17, 2022, FERC filed a NOPR regarding the development of new or modified Reliability Standards to address reliability risks related to inverter-based resources. Specifically, data sharing; model validation; planning and operational studies; and performance requirements for inverter-based resources.
- On Nov. 17, 2022, FERC issued an order regarding the registration of inverter-based resources (IBRs). Specifically, FERC directs NERC to submit a work plan to FERC detailing "how it plans to identify and register owners and operators of IBRs that are connected to the Bulk-Power System, but are not currently required to register with NERC under the bulk electric system (BES) definition."
- On Nov. 17, 2022, FERC issued an order approving Reliability Standards FAC-001-4 and FAC-002-4.

Notable NERC Filings

In October-November, NERC filed the following with FERC:

- On Oct. 13, 2022, NERC and the Regional Entities (ERO Enterprise) submitted comments regarding FERC's notice of proposed rulemaking (NOPR) focusing on improvements to generator interconnection agreements. The ERO Enterprise comments support FERC's efforts to update the Commission's interconnection process with certain important revisions which NERC discusses in its comment.
- On Oct. 28, 2022, the ERO Enterprise submitted a petition for approval of Reliability Standards EOP-011-3 and EOP-012-1. These proposed standards would add to the suite of standards crafted to address the grid risks posed by extreme cold weather. The filing provides the following summary of the proposed EOP-012-1: "[p]roposed Reliability Standard EOP-012-1 is a new Reliability Standard that builds on the cold weather preparedness plan and training requirements currently found in Reliability Standard EOP-011-2 to form a more comprehensive framework for advancing the reliability of the BPS through improved generator cold weather preparedness."
- On Nov. 7, 2022, the ERO Enterprise submitted comments on the FERC NOPR regarding incentive-based rate treatments for voluntary cybersecurity investments.

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	
Jan. 1, 2023	TPL-007-4 – Transmission System Planned Performance for Geomagnetic Disturbance Events (Requirements R3, R4, 4.1, 4.1.1-4.1.2, 4.2, 4.3, 4.3.1, R8, 8.1, 8.1.1-8.1.2, 8.2, 8.3, and 8.3.1)
April 1, 2023	EOP-011-2 – Emergency Preparedness and Operations; IRO-010-4 – Reliability Coordinator Data Specification and Collection; TOP-003-5 – Operation Reliability Data
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

These effective dates can be found here.

Watt's Up at RF

Outreach Recap

ReliabilityFirst 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 avoid holidays).

Our calendar of upcoming events, with agendas and the Webex link to join, can be found on our website, rfirst.org. We will continue to offer engaging topics and speakers throughout 2023.

Some of the speakers this quarter included:

- Kal Ayoub, FERC Deputy Director, Division of Cyber Security, presented on recent reliability related activities, including information on the joint federal-state task force on electric transmission, FERC technical conferences, extreme weather actions, notices of proposed rulemaking (NOPRs) and additional reliability orders.
- Andrew Bochman, Idaho National Laboratory Senior Grid Strategist, presented on small modular reactors, a relatively new technology being tested.
- Tony Jablonski, RF Manager of Risk Analysis and Mitigation, provided an update on the Align tool.
- Rich Bauer, NERC Associate Principal Engineer, RAPA/Event Analysis, presented on Reliability Vignettes, a new product aimed at capturing current operating incidents of interest and projecting the circumstances of the incidents into the future as think pieces for system planning and operating considerations.
- Mallory Carlone, RF Technical Auditor, Operations & Planning, reviewed field walkdowns RF conducted throughout 2022 and the focus for 2023 audit engagements.
- Maria Robinson, director of the Department of Energy (DOE) Grid Deployment Office, discussed the Inflation Reduction Act and Bipartisan Infrastructure Law. Her presentation highlighted tax credits and investment opportunities impacting the electricity sector, including clean energy, expanded transmission and electrification of consumer vehicles.
- Max Reisinger, RF Senior Counsel, Enforcement, presented on the self-reporting process in Align with an explanation of what RF expects to be submitted within each field. He described what makes a good self-report and why RF needs the information requested.

If you missed any past Technical Talks with RF, the presentations can be found on our website under "Technical Talk with RF."

Upcoming January 2023 Technical Talk with RF

Join us for our upcoming Technical Talk with RF on Monday, Jan. 23, 2023, from 2 – 3:30 p.m. The presentations will include a 2023 kickoff and RF Strategic Plan update from Jeff Craigo, RF Senior Vice President of Reliability and Risk, and Diane Holder, RF Vice President of Entity Engagement and Corporate Services.

In addition, Tim Fryfogle, RF Principal Engineer, Engineering and System Performance, will share results of the NERC Winter Reliability Assessment and Long Term Reliability Assessment (LTRA), plus ReliabilityFirst's Winter and LTRA Assessments.

Other upcoming events

Technical Talk with RF | Feb. 13, 2023

Internal Controls Workshop | Feb. 23, 2023

Watt's Up at RF

Gallagher, Burkey discuss tips for organizational cybersecurity posture in GridSecCon keynotes

Tim Gallagher | Joanna Burkey

NERC, E-ISAC and RF hosted the 11th annual Grid Security Conference (GridSecCon), which drew more than 750 virtual attendees from across North America in October. Topics included grid security and planning and preparedness.

RF President and CEO Tim Gallagher opened the three-day conference with a keynote address in which he focused on how good companies can fall into a poor security posture. Joanna Burkey, Chief Information Security Officer at HP, Inc. and member of the RF Board, added her thoughts on how to avoid these pitfalls from her perspective as a cybersecurity practitioner in her keynote speech, which followed Gallagher's on the first day of the conference.

GRIDSECCON 2022
NERC • E-ISAC • RELIABILITYFIRST

RF hosts ERO EG and CCC meetings

The ERO Enforcement Collaboration Group (EG), which includes representatives from all six Regional Entities and NERC, and the Compliance and Certification Committee (CCC), a NERC Board-appointed stakeholder committee, met in-person in October at RF's offices in Cleveland. The EG meets regularly to develop and discuss ERO-wide initiatives and processes to ensure effective, efficient and consistent implementation of the delegated functions. The EG works closely with the other collaboration groups and provides expertise and strategic leadership through enforcement activities. The CCC supports and advises NERC on compliance monitoring and enforcement, registration and certification. During the CCC's October meeting, the EG presented on the lifecycle of a violation, providing insight into the Regions' processes for assessing risk, analyzing mitigation and resolving noncompliance.

Gallagher speaks at OPSI annual meeting

RF President and CEO Tim Gallagher attended the Organization of PJM States, Inc. (OPSI)'s annual meeting in Indianapolis in October and participated in a panel discussion featuring NERC President and CEO Jim Robb as well as state commissioners and policymakers.

RF volunteers at food bank

Eight RF staff members spent the morning of Dec. 9 packing boxes of food and water at the Greater Cleveland Food Bank that will be distributed in the community.


Happy Holidays from RF

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

Forward Together RF ReliabilityFirst

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