PUBLIC

RELIABILITY FIRST

Issue 1 | 2023 Q1

Regulatory Excellence

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,

We are already three months into 2023 and it feels like time is flying by. Thank you to all who have engaged with our outreach events and webinars so far this year from our Ohio Security Tabletop to our Internal Controls Workshop to our State Energy Policy Webinar and beyond. You can read more about these events in this issue if you weren't able to join us for them. When it comes to the work we do, I see these offerings as a vital piece of the puzzle.

In 2023, you will hear a lot from us about our 2023-2027 Strategic Plan, which our executive team introduced to you at January's Technical Talk with RF. This is not only because I am proud of the direction we are heading, but also because we want to be intentional and transparent about how we plan to get there, which I feel is important as your regulator.

This issue is all about "Regulatory Excellence," which is one of our three key objectives in this plan. We talk a lot about the outreach work we do, but this objective is central to our core mission in why we exist and I take it very seriously.

In Continuous Improvement, we will delve into the question of what makes a regulator excellent and how we can all strive to be better in our mission to keep the grid reliable and secure each day through the work we do. You will also read a very special 50th edition of The Lighthouse by Lew Folkerth, in which he discusses how to excel at a CIP audit. I want to congratulate Lew for this monumental achievement and thank him for all the work he has put in to help guide our entities on their journey to CIP compliance.

As Lew puts it so well, at RF we can't steer your ship for you, but we hope by engaging with our Tech Talks and other webinars, attending our events and reading this newsletter, we can be your metaphorical lighthouse, guiding you to take the necessary steps to keep the lights on through the turbulent waters we must constantly navigate.

Forward Together,

Tim

Issue 4 | 2022 Q4

INSIDE THIS ISSUE

Follow us on:

From the Board

Lesley Evancho

Scott Hipkins

RF is pleased to have Lesley Evancho and Scott Hipkins officially on our Board of Directors. Mr. Hipkins has been working with us since he was appointed in August, and the members elected him and Ms. Evancho at the Q4 2022 board meeting.

Lesley Evancho was elected as an independent director and brings with her a wealth of expertise in human capital planning, total rewards, talent management and culture. Ms. Evancho serves as the Chief Human Resources Officer for EQT, which is one of the largest natural gas producers in the country. Previously she was the Vice President of Global Talent Management and Corporate Human Resources at Westinghouse Electric Company, and prior to that she held a variety of human resource roles at Thermo Fisher Scientific, Rice Energy and MSA Safety.

Scott Hipkins was elected as a director for the Transmission Sector and brings with him a wealth of leadership experience in IT operations, Cyber Security and NERC CIP Compliance. Mr. Hipkins is currently the Vice President of Cyber Security and Chief Information Security Officer at FirstEnergy Corporation and previously served in various IT roles and leadership positions at FirstEnergy Service Company.

Since Ms. Evancho and Mr. Hipkins joined the board, we have welcomed them to our offices for their onboarding training and they have been busy working with our staff and their board committees.

We look forward to spotlighting them both in future issues.

2023 Q1-2

ReliabilityFirst

Board of Directors

and Committee

Meetings

will be held

April 26-27, 2023 at the

RF offices.

Click Here

Strategic Plan: Be an Excellent Regulator

A letter from Senior Vice President Jeff Craigo

Dear RF stakeholders,

It is my privilege to share information with you about RF's new strategic plan, which will guide our activities to advance reliability, security and resilience in our footprint over the next five years. The strategic plan has three main objectives: be an excellent regulator, cultivate a highly engaged talented workforce, and harness knowledge to comprehensively address risk. We will focus on each of these objectives over the next several newsletter issues.

The first objective, to be an excellent regulator, is one of the core responsibilities. We broke down this responsibility into three more specific objectives, which are: 1) Consistently demonstrate accountability and transparency through our model; 2) Commit resources to collaboration and security; 3) Build deep knowledge of our entities and use it to serve our footprint.

In the first year of the plan, we already have many efforts underway that will allow us to leverage our brilliant model. We've been working closely with the ERO, participating in over a dozen task forces and collaboration groups. These groups focus on improving reliability, security and resilience through issuing implementation guidance and technical whitepapers, creating industry guidance documents and practice guides, standardizing processes both internally and with stakeholders, and helping entities prepare for new or revised NERC Reliability Standards. Examples of these collaborative efforts include activities for sustaining facility ratings, improving protection system misoperation rates, expanding the use of internal controls, performing more complex energy assessments, and improving preparedness for extreme cold weather.

In terms of security, we continue to focus on improving our internal security practices and systems that safeguard internal data and information. We also continue the implementation of Align in parallel with the Secure Evidence Locker (SEL) that helps secure an environment to manage our compliance monitoring and enforcement processes.

And we are always working to better understand our entities and improve the value of our offerings. Last month we hosted our internal controls workshop, which we will discuss later in this issue. We also conducted our first state tabletop security exercise with a goal of improving disaster and emergency response by strengthening communication channels between critical infrastructure providers, government partners, and the community.

Striving to be an excellent regulator is the first objective of our strategic plan and is at the core of our mission, which is serving the public good and supporting health and safety through preserving the reliability, security and resilience of the grid.

Forward Together,

Jeff Craigo, Senior Vice President

Continuous Improvement

By Sam Ciccone, Principal Reliability Consultant

Regulatory Excellence

The Journey to Security, Resiliency and Reliability

"We will chase perfection, and we will chase it relentlessly, knowing all the while we can never attain it. But along the way, we shall catch excellence."

— Vince Lombardi, NFL Hall of Fame head coach and namesake of the Super Bowl trophy

When the Kansas City Chiefs raised the Lombardi trophy in Super Bowl LVII, it was a culmination of months of preparation, discipline, determination, conquering adversity and improving their game plans and personnel. They weren't perfect by any means. They didn't win all 17 regular season games. They allowed teams to score on them during the season and during the playoffs. Most, if not all of the team played with injuries. But as they battled on that field that Sunday, they achieved excellence.

Similarly, the Electric Reliability Organization (ERO, collectively NERC and the Regions), has been on its own path of continuous improvement as we strive for excellence in regulation. In 2014, we introduced the Reliability Assurance Initiative. We began focusing on internal controls and introduced new tools such as self-logging. The ERO continues to evolve today with our educational and outreach offerings, E-learning modules, and Assist Visit program to help combat risks to reliability and security. Our evolution has led to new initiatives such as state outreach, plus our online self-assessment tools to measure resilience, detect insider threats, and implement security-based tabletops.

What makes a regulator excellent?

When I think about this question, I believe Cary Coglianese's Listening, Learning, and Leading: A Framework for Regulatory Excellence is instructive. There are certain core principles that make an excellent regulator, according to Coglianese, a University of Pennsylvania professor and founding director of the Penn Program on Regulation.

One of the most important characteristics of a regulator is transparency, Coglianese writes. At RF, we created the Assist Visit program several years ago to offer transparent compliance, reliability and security guidance, and many entities have benefited from this program by meeting with us to discuss implementation guidelines, internal controls, and follow-ups to recommendations and areas of concern from audit.

Another key attribute is competence, and RF's knowledgeable staff is central to our mission of excellence in regulation. For the ERO, it's not enough to be subject matter experts in operations and planning and cyber and physical security. We need to know our entities and industry risks inside and out. This aligns with RF's 2023-2027 Strategic Plan, which states *"RF works closely with the entities in our critical and unique Region to build a deep knowledge of our footprint."* With this outlook in mind, RF strives to be a good listener to industry as well, formulating what we are hearing to adjust how we regulate. Through committees and standards drafting teams, entities can have direct input on how they are regulated.

Analytical capability also comes into play. This has been an improvement at RF and the ERO, as we have developed dashboards to measure and analyze our footprint through various metrics, helping us better communicate risk to our stakeholders.

And perhaps most important of all, Coglianese emphasizes that a regulator exists to serve the public interest. RF serves the public good and supports health and safety through preserving and enhancing the reliability, security and resilience of the grid. In service of this mission, we use the Compliance Monitoring and Enforcement Program (CMEP) to help drive industry toward continuous improvement and also offer our subject matter expertise as a

Continued on page 6

Continuous Improvement

Continued from page 5

resource to the states and communities in our footprint.

How can CI concepts drive regulatory excellence?

The Define, Measure, Analyze, Improve, and Control (DMAIC)[1] Continuous Improvement (CI) model can be used in a vast array of CI initiatives, and it also applies to regulatory excellence:

Define – How does the regulator define excellence? In our industry, is it defined as keeping the lights on? Is it ensuring our entities are meeting their compliance obligations? Is it providing guidance to entities in many different forums in the interest of reliability? Is it having a highly knowledgeable staff? Is it having a risk-based focus on compliance? The answer is: yes, all of these, and more. As Bridget M. Hutter, professor of risk regulation at the London School of Economics and Political Science, puts it: *"excellent regulators are those who appreciate both the limitations of the data and the political context within which they operate."*

Measure and Analyze – Coglianese discusses measuring the current state as a regulator. He says: "*with a sufficiently funded and highly trained staff working in a supportive organizational culture, an excellent regulator uses the best tools and technologies available to solve problems and it earnestly seeks continuous improvement through regular performance measurement and evaluation*." This aligns with RF's strategic plan, in which RF President and CEO Tim Gallagher states, *"we are fortunate to have a brilliant model for the ERO that inherently provides accountability and affords us access to an incredible amount of data and benchmarking opportunities.*"

Improve – As we offer our entities tools and information for improvement, we, the regulator, must also improve. Continuous improvement keeps the machine moving during various changes in the regulatory environment. As Isabel Villanueva, head of the cabinet of the secretary general in Spain's Nuclear Safety Council puts it, "*continuous improvement is a key goal for regulators and there should be no room for complacency in achieving it."*

Control – This can be thought of as sustainability. How do you sustain regulatory excellence? One of the ways to maintain excellence is through the people, which RF also prioritizes as a core objective in our Strategic Plan. In this case, sustainability means ensuring you have the competent and knowledgeable personnel for the long-term, meaning you can't just rely on current high performers, but must also make sure the organization works to achieve continuity in the long-term performance of its workforce. RF, like the industry, is working on building bench strength and ensuring sustainable programs that focus on raising capabilities without relying on a single high-performer or expert. Control also includes governance or ensuring the DMAIC cycle stays on track. Without sustained management oversight, the continuous improvement process can falter.

Conclusion

Perfection, in any phase of life, is not practical. It takes an assessment of the current state to determine a goal for improvement to achieve excellence. We as regulators are dedicated to improvement, and in turn, we hope our improvement drives you to pursue excellence. Our CI journey only works if you, our entities, are equally invested in working with us (e.g., participating in assist visits, self-assessments, demonstrating internal controls during audit, working with the Risk Analysis & Mitigation team on sustainable mitigation plans). We know that neither the ERO nor our entities are perfect, but we must always chase improvement. And in so doing, we hope to be like Vince Lombardi and catch excellence.

---

[1]DMAIC methodology consists of five phases, namely, Define, Measure, Analyze, Improve, and Control. These phases form the pillars of the DMAIC framework, allowing us to improve an existing business function or an entire organization to achieve improvement and effectiveness https://www.6sigma.us/dmaic-process/.

The Lighthouse

By Lew Folkerth, Principal Reliability Consultant

How to Excel at a CIP Audit

Your path to an excellent CIP audit begins with an excellent operational security program, which means your security program must exceed the Requirements of the CIP Standards. Keep in mind that the CIP Standards are intended as a baseline that all Responsible Entities must meet. If you do not exceed that baseline, you are almost certainly leaving your systems exposed to unnecessary risk.

I have provided, and will continue to provide, pointers on how to improve your security program in other articles in this series, but now let's concentrate on how you demonstrate your excellent security program to an audit team.

In order to document and maintain an excellent security program, you must also have an excellent compliance program. The true function of a compliance program is to monitor and document your security program. In addition, an excellent compliance program will help your security program "adapt to shifting environments, evolving demands, changing risks, and new priorities" (from GAO-14-704G Federal Internal Control Standards, Page 1). This is the definition of an internal controls program.

What I'm saying here is that an excellent compliance program is really an excellent internal controls program with some additional functions to generate compliance evidence. See Figure 1 for how this should work.

Figure 1 (on the next page) shows my concept of a modern compliance system and how it may be audited. The Compliance Audit will consist of a review of the compliance evidence. To help obtain reasonable assurance of compliance, the Internal Controls Assessment may review the internal controls associated with the Requirement being reviewed.

If the internal controls are strong and comprehensive, this will add strength to the compliance evidence. The Security Risk Review will assess the effectiveness of your security controls in protecting your systems. This assessment may reference published guidance, security guidelines, accepted security practice, and other sources to ensure a valid review.

With the foundation of an excellent security program monitored by an excellent internal controls program and documented by an excellent compliance program, you should be well on your way to achieving excellence at audit. To make the most of these foundations I want to ensure that you understand the basics of an audit and are ready to supply the information an audit team will need to obtain reasonable assurance of your compliance.

Audit Concepts

To excel at a CIP audit, you need to understand what information the audit team is looking for and provide that information in a clear, concise manner. Compliance audits are performed according to the Generally Accepted Government Auditing Standards (GAGAS, available here).

When you read GAGAS you can ignore Chapters 6 and 7, as these do not

White River Light Station, White Hall, Michigan – Photo: Lew Folkerth

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.

Continued on page 8

Continued from page 7

pertain to a Performance Audit. In reading Chapter 8, Fieldwork Standards for Performance Audits, you should understand these concepts.

Sufficient, appropriate evidence:

Evidence is the key to a successful audit. Your goal in submitting evidence is to provide the audit team with reasonable assurance that you are complying with the Requirement in question. In most cases the CIP Evidence Request Tool (ERT) will be your guide to gathering, formatting and submitting evidence. Auditors must obtain sufficient, appropriate evidence to support their conclusions.

Appropriate evidence is relevant, valid and reliable. Sufficient evidence provides enough appropriate evidence to address the audit objectives and

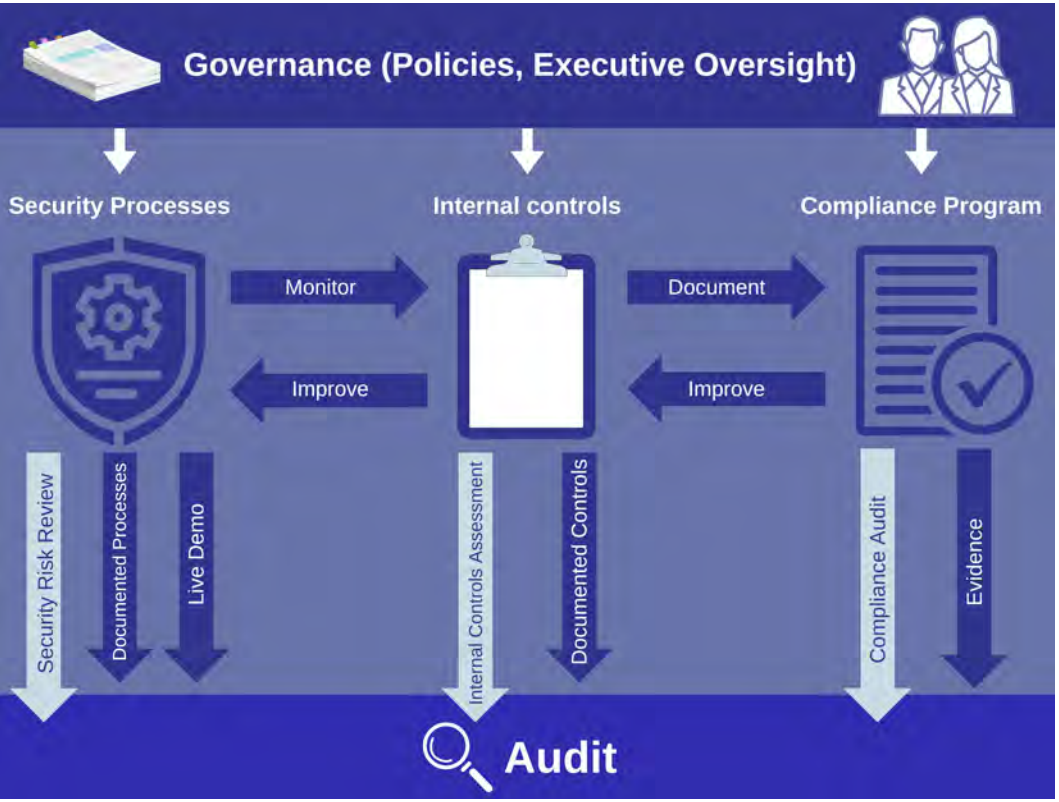


Figure 1

to support the findings of the audit team. Evidence from more than one source may be used to support the audit team's review. This is known as "stacking evidence."

Effective evidence is also clear, complete and concise. It should clearly demonstrate compliance with the Requirement. It should be complete, so the audit team doesn't need to request additional evidence, and it should be concise to eliminate unnecessary information. Another way of looking at effective evidence is that it should tell the story of how you maintain compliance with the Requirement.

Your narrative of how you perform this task can be included in the Reliability Standard Auditor Worksheet (RSAW) in the Compliance Narrative section for the applicable Requirement or Part.

Professional judgment:

Auditors are expected to use professional judgment when reviewing your performance. Professional judgment includes exercising reasonable care (acting in accordance with professional standards and ethical principles) and professional skepticism (having a questioning mind, awareness of relevant conditions, and performing a critical assessment of evidence).

This means you need to give the auditors confidence in your ability to protect your CIP assets and maintain reliability, resilience and security. You establish your credibility with the audit team by being open and forthcoming. You and your SMEs should be proud of what you do, and that pride should show in your interactions with the audit team.

The audit team

Your audit team will consist of an Audit Team Lead (ATL), one or more sub-teams, and possibly observers. The ATL is your point of contact for all things related to the audit. Each sub-team will have at least a lead and a scribe. The sub-team lead guides the review of the sub-team's assigned Requirements. The scribe documents the review and coordinates additional evidence requests. Observers may include staff or management from FERC, NERC or Regions. The observers may vary in their level of participation, but in no case does an observer influence the team's findings.

Contrary to popular belief, an ERO Enterprise audit team's primary purpose is to find you compliant with the Standards and will work with you if necessary to help you demonstrate compliance. It is only when this joint effort fails that an audit finding will result. As SERC's Robert Vaughn says in

Continued on page 9

Continued from page 8

"Your audit team is a team of seasoned professionals with diverse backgrounds in cybersecurity, including patch management, remote access, physical security, etc. They are available to answer questions and help walk you through the process. Please work directly with them regarding expectations for when they arrive on site regarding the agenda, anticipated questions, and discussion points to ensure that the right SMEs are present to lead discussions and demonstrate your programs. Please pick venues that match the time, duration and needs for the discussions including appropriate A/V settings and a table/chair setup that is conducive to the upcoming conversations."

Brian Thiry
RF Director and former O&P Auditor

"Good documentation is auditor kryptonite."

Robert Vaughn
CIP Auditor, SERC

the sidebar quote, good documentation is essential to a good outcome.

Remember to keep the audit at a conversational and cooperative level to achieve the best results. (See "Defense Against the Dark Auditor," Lighthouse #22, Sep/Oct 2017, available here.)

The audit process

The audit will begin with an opening briefing by the ATL, followed by your opening presentation. It will be helpful, but not essential, to have your presentation delivered by a senior executive. This helps demonstrate executive commitment to the operational cyber security program. The major portion of the audit will be subject matter expert (SME) interviews and site visits. The ATL will close out the on-site portion of the audit with a preliminary exit briefing.

During the audit it is essential to get the right SMEs in front of the auditors. The SMEs you choose should be the people who actually do the work of implementing your security processes. Your SMEs should be briefed on what to expect and should understand that their interaction with the auditors will be interviews, not testimony. The interviews should be conducted as a conversation and should not be confrontational. Your SMEs should be open and honest with the audit team to establish their credibility. During their interviews, they should:

- Describe how security processes are followed;
- Show how the security processes protect your systems and meet compliance requirements;
- Show how documented internal controls ensure consistency and sustainability in these processes; and
- Explain how the evidence demonstrates that the processes are performed without exception. In complex cases, you may want an SME to perform a live demo of a system to show how it functions.

Another key to a successful compliance audit is constant audit readiness. According to the Compliance Monitoring and Enforcement Program (CMEP, NERC Rules of Procedure Attachment 4C) Section 4.1.2, an unscheduled audit can be initiated with a prior notification of 10 business days. If your processes are not in constant readiness to produce compliance evidence, you will have a very rough time if an unscheduled audit of your entity is initiated.

Audit findings

During the exit briefing, you will be given the preliminary results of your audit. Here are the possible audit findings, coupled with my understanding of their current meaning:

- Potential Noncompliance (PNC) – The audit team has not been able to obtain reasonable assurance that you are in compliance with the Requirement cited. A PNC, if sustained by RF Management and Enforcement reviews, will enter you into the Enforcement and Mitigation processes.
- Area of Concern (AoC) – The audit team is concerned that your compliance with the cited Requirement may not be sustainable or effective in adequately protecting your systems.
- Recommendation – An audit team suggestion to improve your program.
- Positive Observation – The audit team's feedback to you on things you are doing particularly well.

Continued on page 10

Continued from page 9

Audit tools

Be familiar with the tools the auditors will use. Unlike other types of audits, you are provided with a full list of information the auditors will ask for, making an audit more like an open-book test. Here are the tools you will need:

- Align – Organizes the information about your entity and facilitates the compliance engagement.
- Secure Evidence Locker (SEL) – Stores your compliance evidence during the audit.
- Reliability Standard Auditor Worksheet (RSAW) – Auditor tool used to organize the review of your evidence. The compliance narrative section is used for you to tell your story of how you approach compliance with a Requirement or Part. The narrative should be informative but concise.
- CIP Evidence Request Tool (ERT) – Tells what evidence is needed and establishes populations of evidence for sampling. The ERT is available here, and the ERT User Guide is here.

Conclusion

"Our overall goal as auditors is to have reasonable assurance that you have a sound security program. We do this through the evidence review process and asking questions around your internal controls program. We ask that you concisely tell your compliance story on engagements and that you demonstrate the pride you have in your program as we want to see you going above the standards."

Jim Kubrak, RF Manager, O&P Compliance Monitoring, and
Zack Brinkman, RF Manager, CIP Compliance Monitoring

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.

Be sure to request any assistance you want well before your audit begins. Your audit becomes active when you receive the audit notification letter and remains active until your exit briefing.

During the time your audit is active, RF is restricted in how we can assist you. In particular, the Assist Visit program will be unavailable to you during your audit period.

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

Coda

On this occasion of the 50th issue of The Lighthouse, I wish to thank all the people who have made this series possible. As with any ERO document, it is not the product of just one person. While I am solely responsible for the content of each article, I wish to thank those who have contributed to the success of this column over the years. I thank my publication staff and my review teams: technical, legal and editorial.

And my thanks to RF as a whole for providing me this opportunity.

Lew Folkerth and Entity Engagement Director Brian Thiry

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

RF takes innovative approach to Internal Controls Workshop

RF Technical Auditors Lindsey Mannion (left) and Courtney Fasca organized and hosted the workshop.

RF President and CEO Tim Gallagher

ReliabilityFirst hosted an Internal Controls Workshop on Feb. 23 in Cleveland, Ohio, for entities. We took an innovative approach to a full-day workshop; rather than filling the day with multiple PowerPoints, this workshop concentrated on interactive activities encouraging collaboration, which resulted in learning opportunities for all on how a sound controls program enhances organizations' mitigation of risk.

The workshop concentrated on FAC-008, CIP-005 and CIP-007, but internal controls can be applied everywhere. Many of the techniques described could be applied to a multitude of standards.

The day began with opening remarks from RF President & CEO Tim Gallagher, highlighting the importance of internal controls and their place in our industry.

The attendees ranged from those who have worked with internal controls for several days, to several years, to several decades. To level-set the room, we went over common terminology that would be used throughout the workshop in our "What is a Control?" session. For the 2023 workshop, we decided to use the example framework in the GAO Green Book and utilized its principles throughout the sessions. Our first activity was "Finding Controls in Everyday Life," where participants identified preventive, detective, and corrective controls in common objects – even in something as simple as an egg carton.

The RF Risk Analysis & Mitigation (RAM) team presented methods to map and address risks, pointing out potential areas for controls and highlighting examples of control failure points they have seen. They reminded the audience that internal controls are one of the seven ERO Performance Considerations in Compliance Oversight Plans (COPs).

Our next activity, "Addressing the Risk," was an extended metaphor for the importance of layering controls. During the activity, participants layered controls to mitigate waves of risk, realizing that overreliance on a key control activity or general complacency can lead to failure.

Taking a break from the group activities, the RF staff performed an interactive skit. Attendees voted on different turning points of the play, driving conversations regarding internal controls discussions on real

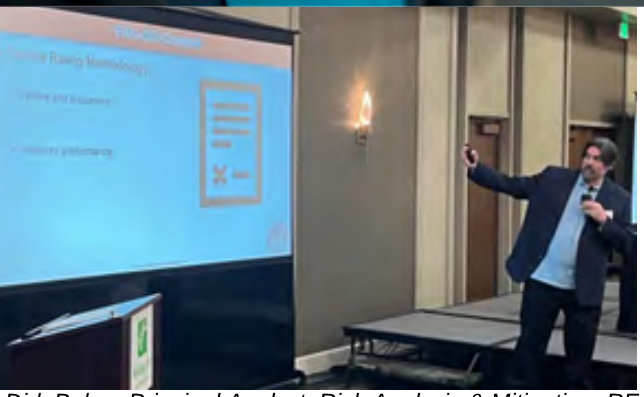
"Finding Controls in Everyday Life" activity

"Finding Controls in Everyday Life" activity

Continued on page 12

Internal Controls

Continued from page 11



Dirk Baker, Principal Analyst, Risk Analysis & Mitigation, RF

RF Compliance Monitoring team members Jim Kubrak, Ash Chappell and Courtney Fasca, participate in an internal controls skit.

Alan Herd, FERC

topics, such as winterization and post-event analysis.

After taking a quick lunch break, the attendees participated in a “Compliance Drill” activity, addressing fictional operational events and a CIP security threat. This underscored how creating and monitoring different control activities improves ongoing reliability and security.

Alan Herd, the manager of CIP compliance monitoring for the Office of Electric Reliability at FERC, held a discussion and Q&A session highlighting the importance of internal controls in our industry.

The final activity focused on using that GAO Green Book example framework, demonstrating that an internal controls program is not a one-and-done, not one-size-fits-all. Rather, a good internal controls program is an ongoing and continuous effort. An internal controls program is comprised of more than just control activities.

A strong internal controls program establishes responsibilities (“tone at the top”), assesses targeted risks, codifies the information flow and communication beyond a single business unit, and includes a monitoring piece that ensures continuous improvement and effective implementation.

Remember, you can say you have all these fancy controls, these automatic processes, a beautiful shiny car… but does it work for the benefit of your organization? Is there even an engine? A brake system? It needs to work, not just look great on paper.

As we continue to emphasize the need for excellence and sustainability, focus on your company’s security and reliability risks and what controls you can put in place to enhance your program. Internal controls are an inherent part of the audit process, but most importantly, a key part of ongoing reliability.

"Addressing the Risk" activity

"Addressing the Risk" activity

Enforcement Explained

By: Mike Hattery, Counsel

Physical Security Common Failure Points

Physical security is a constant concern at ReliabilityFirst and the ERO at large, but it has been thrust to the forefront of national discussion of late following attacks on multiple substations. Here we'll explore some common failure points that we are seeing in the physical security space in terms of both preventive controls and breach identification controls.

Taking a proactive approach to preventative controls is essential

The central requirements for entity physical security plans and protections for Physical Security Perimeters (PSPs) rest in CIP-006-6, and elevated requirements around certain transmission stations, substations and primary control centers rest in CIP-014-3. Additionally, requirements for low-impact sites rest in CIP-003-8.

Specifically, when it comes to CIP-006-6 R1.1-R1.3, one of the most common issues we see is Physical Access Controls Systems (PACS) failing, and as a result, adversely impacting PSP security. We've seen this come up during a transition to backup power (i.e., loss of primary power supply) or after a PACS restart (e.g., can occur due to power disruption, during transition to backup power, or following maintenance). In these scenarios, the PACS failure typically results from delayed or fragmented restarts.

It is important for a registered entity to understand how access points will function in these scenarios (e.g., fail safe versus fail secure). Another issue in device restarts that can arise is, when restored, sometimes the settings can revert to prior versions creating incompatibility or a lack of correct access lists.

This is where CIP-006-6 R3.1 maintenance and testing function as such an important control. Testing PACS at least every two years is essential, and a proactive entity will test PACS with more frequency and in varying scenarios (i.e., after a cold restart or some other disruptive event). Another useful tool is utilizing security walkdowns of facilities to test different PACS devices and access controls to assure functionality.

An effective walkdown might include testing PSP doors to ensure they are closed and secured, prompting alarms to see if they function as intended and reviewing camera angles to assure they are capturing appropriate areas. Adding surface-level PACS testing to physical security walkdown checklists is a solid step in improving the probability that a non-functional PACS will be identified and remediated quickly.

Continued on page 14

Enforcement Explained

Continued from page 13

When it comes to CIP-014-3, we've identified some shortcomings in R1 risk assessments through our compliance monitoring and enforcement activities (e.g., scope of facilities and contingencies studied).

These shortcomings can create issues when it comes to identifying and protecting critical facilities, so we encourage registered entities to proactively evaluate their approach to R1 risk assessments and reach out to our Entity Engagement team if they have questions regarding their approach to CIP-014-3 analysis, as opposed to waiting for a compliance monitoring engagement. And, as far as reducing the overall risk to the Bulk Electric System, it is worth highlighting that ReliabilityFirst has observed some registered entities adopt a best practice approach of implementing heightened physical security protections at more facilities.

Contact Entity Engagement

We encourage registered entities to proactively evaluate their approach to R1 risk assessments and reach out to our Entity Engagement team if they have questions regarding their approach to CIP-014-3 analysis.

Do not fall victim to alarm apathy

Increasingly, being nimble in terms of limiting damage and executing expedited restoration requires near instantaneous response to alarms indicating a potential breach attempt. One of the root causes or fact patterns of concern for ReliabilityFirst relates to alarm apathy. For several entities in the ReliabilityFirst footprint, central security will encounter a number of false positive alarms for PSPs on a daily basis (including remote locations where deployment may be necessary).

This is a physical security struggle that Aesop's "The Boy Who Cried Wolf" foretold, constant alarms and notifications leading to an atrophy of attention for when the actual wolf (attempted breach) appears.

One of the points well-articulated in February's Technical Talk with ReliabilityFirst was that without proactivity in response to alarms, their existence becomes moot. With this in mind, we encourage entities to emphasize the importance of timely investigating all alarms to their security groups and staff at large. Additionally, consider evaluating recent alarm response times, and assess whether more aggressive action needs to be taken. Finally, entities should review their central alarm interface to determine if changes need to be made to alarms or notifications to reduce unnecessary noise.

Vigilance is key

In terms of the failure points discussed above, there is one cultural theme that is essential, vigilance. Entities have to support a culture of vigilance among both their security and non-security staff. Be it performing proactive walkdowns to assure functioning PACS, increased scenario testing for PACS devices, or behaving as if each alarm could be the real thing, doing these things effectively requires a culture of vigilance.

PJM details Resource Retirements, Replacements and Risks

Third phase of energy transition study looks at changes in generation and load through 2030

The third phase of PJM's ongoing study of impacts associated with the energy transition explores the pace of resource retirements and replacements through 2030 and highlights potential reliability risks to meeting growing electricity demand.

Energy Transition in PJM: Resource Retirements, Replacements and Risks (PDF) is the latest study in a multiyear, multiphase effort undertaken in light of industry trends and PJM's strategic focus on helping to facilitate state and federal decarbonization policies reliably and cost-effectively across 13 states and the District of Columbia.

PJM's research highlights four trends below that, in combination, present increasing reliability risks during the transition, due to a potential timing mismatch between resource retirements, load growth and the pace of new generation entry under a possible "low new entry" scenario:

- The growth rate of electricity demand is likely to continue to increase from electrification coupled with the proliferation of high-demand data centers in the region.
- Thermal generators are retiring at a rapid pace due to government and private sector policies as well as economics.
- Retirements are at risk of outpacing the construction of new resources, due to a combination of industry forces, including siting and supply chain, whose long-term impacts are not fully known.
- PJM's interconnection queue is composed primarily of intermittent and limited-duration resources. Given the operating characteristics of these resources, we need multiple megawatts of these resources to replace 1 MW of thermal generation.

The analysis also considers a "high new entry" scenario, where this timing mismatch is avoided. While this is certainly a potential outcome, given the significant policy support for new renewable resources, our analysis of these long-term trends reinforces the importance of PJM's ongoing stakeholder initiatives, including capacity market modifications, interconnection process reform and clean capacity procurement, and the urgency for continued, combined actions to de-risk the future of resource adequacy while striving to facilitate the energy policies in the PJM footprint.

Overall, the amount of generation retirements appears to be more certain than the timely arrival of replacement generation resources and demand response, given that the quantity of retirements is codified in various policy objectives, while the impacts to the pace of new entry of the Inflation Reduction Act, post-pandemic supply chain issues, and other externalities are still not fully understood. Should these trends continue, PJM could face decreasing reserve margins for the first time in its history.

Specifically, the analysis shows that 40 GW of existing generation are at risk of retirement by 2030. This figure is composed of: 6 GW of 2022 deactivations, 6 GW of announced retirements, 25 GW of potential policy-driven retirements and 3 GW of potential economic retirements. Combined, this represents 21% of PJM's current installed capacity.

In addition to the retirements, PJM's long-term load forecast shows demand growth of 1.4% per year for the PJM footprint over the next 10 years. Due to the expansion of highly concentrated clusters of data centers, combined with overall electrification, certain individual zones exhibit more significant demand growth – as high as 7% annually.

On the other side of the balance sheet, PJM's New Services Queue consists primarily of renewables (94%) and gas (6%). Despite the sizable nameplate capacity of renewables in the interconnection queue (290 GW), the historical rate of completion for renewable projects has been approximately 5%.

The projections in this study indicate that the current pace of new entry would be insufficient to keep up with expected retirements and demand growth by 2030. The completion rate (from queue to steel in the ground) would have to increase significantly to maintain required reserve margins.

Continued on page 16

Continued from page 15

In the study, PJM also considers generation entry beyond the queue using projections of higher new entry of resources. Those projections indicate that, despite eroding reserve margins, resource adequacy would be maintained if the influx of renewables materializes at a rapid rate and gas remains the transition fuel, adding 9 GW of capacity. The analysis performed at the Clean Attribute Procurement Senior Task Force (CAPSTF) also suggests that further gas expansion is economic and competitive.

The findings of this study highlight the importance of PJM's ongoing stakeholder initiatives (Resource Adequacy Senior Task Force, Clean Attribute Procurement Senior Task Force, Interconnection Process Subcommittee), continued efforts between PJM and state and federal agencies to manage reliability impacts of policies and regulations, and the urgency for coordinated actions to shape the future of resource adequacy.

In support of this ongoing work, the PJM Board of Managers issued a letter initiating the Critical Issue Fast Path (CIFP) process to tackle the resource adequacy and reliability issues that are currently before stakeholders in the Resource Adequacy Senior Task Force (RASTF). The CIFP is a unique, accelerated stakeholder alternative to the normal stakeholder process designed to expeditiously resolve issues that are contentious or time sensitive.

Background

PJM has undertaken multiple initiatives in coordination with stakeholders and state and federal governments to facilitate the decarbonization policies within its footprint reliably and as cost-effectively as possible and to help build out the grid of the future, including interconnection queue reform, deployment of the State Agreement Approach to facilitate 7,500 MW offshore wind in New Jersey, and coordination with state and federal governments on maintaining system reliability while developing and implementing their specific energy policies.

The first two phases of the energy transition study, Frameworks for Analysis (PDF) and Emerging Characteristics of a Decarbonizing Grid (PDF), focused on energy and ancillary services and resource adequacy in 2035 and beyond. This third phase focuses on resource adequacy in the near-term through 2030.

Regulatory Affairs

Willie Phillips named as FERC's acting chairman

In January, the White House named FERC Commissioner Willie Phillips as FERC's Acting Chairman. Chairman Phillips joined FERC in December 2021 and is the first African American to lead FERC. He previously served as Chairman of the Public Service Commission of the District of Columbia. He also worked as an attorney at NERC for several years.

During his first meeting as FERC Chairman, he discussed his priorities for FERC, including reliability, transmission and diversity/equity. He stated that reliability is "job number one," and discussed threats related to cyber and physical security and extreme weather. Chairman Phillips also discussed the importance of incentivizing smart transmission investments, while reducing costs and ensuring reliability. When discussing diversity and equity, he noted that FERC will be convening a roundtable on environmental justice and equity.

FERC issues order on Internal Network Security Monitoring

On January 19, FERC issued Order 887, "Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems." The order directs NERC to strengthen the CIP Standards by requiring internal network security monitoring (INSM) for all high-impact BES cyber systems and certain medium impact BES Cyber Systems. INSM is a subset of network security monitoring applied within a "trust zone," such as an Electronic Security Perimeter. INSM provides an additional layer of protection by providing visibility over communications between networked devices within a trust zone, and detecting malicious activity that has breached perimeter network defenses. Order 887 states that entities need to:

- Develop baselines of their network traffic inside their CIP-networked environment
- Monitor for and detect unauthorized activity, connections, devices and software inside the CIP-networked environment
- Identify anomalous activity to a high level of confidence by: (1) logging network traffic; (2) maintaining logs/data collected regarding network traffic; and (3) implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques and procedures from compromised devices

Order 887 also directs NERC to study the risks posed by a lack of INSM, and submit a report within 12 months on the feasibility of implementing INSM at low impact BES Cyber Systems and medium impact BES Cyber Systems without external routable connectivity.

FERC approves two cold weather standards, directs modifications

On February 16, FERC issued an order which approves two new cold weather reliability standards: EOP-011-3 (Emergency Operations) and EOP-012-1 (Extreme Cold Weather Preparedness and Operations). The order approves both standards as just and reasonable, and directs NERC to develop and submit modifications to EOP-012-1 to:

- Ensure the applicability criteria captures all BES generation needed for reliable operation during freezing conditions
- Modify R1 and R7 language regarding when generators may declare "technical, commercial, or operational constraints" that would exempt them from implementing required freeze protection measures (and clarify how that declaration and exemption process would work)
- Modify R1 to ensure that generators that are incapable of operating for 12 continuous hours (like solar facilities during winter months) are not excluded from compliance
- Modify R2 to require that freeze protections allow equipment to operate for a longer period of time than one hour
- Modify R7 to include deadlines for completion of corrective action plans
- Shorten the 60-month implementation plan for existing generating units

DOE releases annual summary of emergency incidents and disturbances

The Department of Energy (DOE) recently released its annual summary of electric emergency incidents and disturbances reported through Form OE-417, and the data shows a 77% increase in the number of physical attacks on the grid from 2021 to 2022. Out of the 390 incidents, 163 involved deliberate physical damage to Bulk Power System equipment (up from 92 recorded in 2021).

Winter Storm Elliott joint inquiry underway

FERC, NERC and the Regions are conducting a joint inquiry into the operations of the Bulk Power System (BPS) during the extreme weather that occurred during recent Winter Storm Elliott and contributed to power outages across the country. Although most outages were at the distribution level, there were rolling blackouts in Tennessee and the Carolinas and the BPS was significantly stressed in other regions. The joint inquiry team is working with other federal agencies, states and utilities to identify issues that occurred and potential solutions.

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 2022 Annual Report

In February of 2023, NERC published its 2022 annual report. The annual report addresses a number of items including the expanding risk-based focus in standards. Central on the CIP side are transmission planning and the associated operational cyber risks, and supply chain risk mitigation. On the operations and planning side, the report covers the advances in cold weather standards, a focal point for the ERO.

NERC Publishes CMEP and Registration Annual Report

On Feb. 9, 2023, NERC filed its annual report on CMEP and organization registration and certification programs. On the CMEP side, this report discusses both noncompliances reported in 2022 as well as serious and moderate risk violations filed in 2022. On the organization registration side, the report identifies changes in registration throughout the ERO, including considerable growth in registrations of generator owners and generator operators.

Notable FERC Orders

In January-March, FERC filed the following:

- On Feb. 16, 2023, FERC issued an order approving cold weather reliability standards. The order approves EOP-011-3 (emergency operations) and EOP-012-1 (extreme cold weather preparedness and operations). However, it also directs certain modifications to EOP-012-1.
- On Jan. 19, 2023, FERC issued an order directing NERC to develop a new or modified CIP standard that requires internal network security monitoring for CIP-networked environments for all high impact Bulk Electric System (BES) Cyber Systems with and without external routable connectivity as well as medium impact BES Cyber Systems with external routable connectivity.

Notable NERC Filings

In January-March, NERC filed the following with FERC:

- On Feb. 6, 2023, NERC and the Regional Entities (ERO Enterprise) submitted comments regarding FERC's notice of proposed rulemaking (NOPR) focusing on the reliability risks posed and introduced by the growth of inverter based resources (IBRs).The ERO notes its actions and support for adding among other things: data sharing requirements, model validation requirements and requirements for planning and operational studies.
- On Feb. 15, 2023, NERC submitted a Work Plan regarding the creation of a new registration category to address the increase of IBRs.
- On March 2, 2023, NERC filed a petition with FERC for the approval of PRC-023-6. The proposed version of the standard, if approved, would retire requirement two of the prior versions of PRC-023.
- On March 10, 2023, NERC filed a petition with FERC for the approval of PRC-002-4. The purpose of the proposed revisions is to address two items; (1) addressing impacts associated with the influx of IBRs, and (2) clarifying requirements in terms of notifications as well as when sequence of recording data and fault recording data are required.

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

Items Posted for Comment

Posting	Action	Start Date	End Date
NERC posted a comment period for a draft reliability guideline. Specifically, this reliability guideline is developed to provide suggested approaches for the managing operating reserve.	Submit Comments	3/6/2023	4/20/2023
NERC posted a comment period for a draft white paper. The white paper addresses consideration for performing an energy reliability assessment. The intention is to clarify the energy reliability assessment process and provide elements to analyze when performing an energy reliability assessment.	Submit Comments	3/7/2023	4/21/2023

These effective dates can be found here.

Ohio Security Tabletop brings together critical infrastructure providers for emergency response exercise

ReliabilityFirst (RF) conducted the 2023 Ohio Security Tabletop Exercise simulating a long-term power outage in the Columbus, Ohio, area on Feb. 10. The scenario simulated an electromagnetic pulse (EMP) being set off over the Columbus Airport, with an impact radius of 10 miles.

The overall goal was to conduct a preparation drill to improve disaster and emergency response by strengthening communication channels between critical infrastructure providers, government partners and the community on a local level. This exercise was the first of this type that RF has conducted.

Participants included individuals from healthcare, communications, law enforcement, water utilities, electric utilities, NERC, RF, and local, state and federal government. They practiced emergency management procedures, created relationships to improve information sharing and identified key issues and gaps.

Diane Holder testifies at Pennsylvania State Senate hearing on impacts of Winter Storm Elliott

RF Vice President of Entity Engagement and Corporate Services Diane Holder, PJM Vice President of State and Member Services Asim Haque, and Pennsylvania Public Utility Commission Chair Gladys Brown Dutrieuille served as panelists at the Pennsylvania State Senate Environmental and Consumer Protection Committees' joint hearing on grid reliability and the response to Winter Storm Elliott.

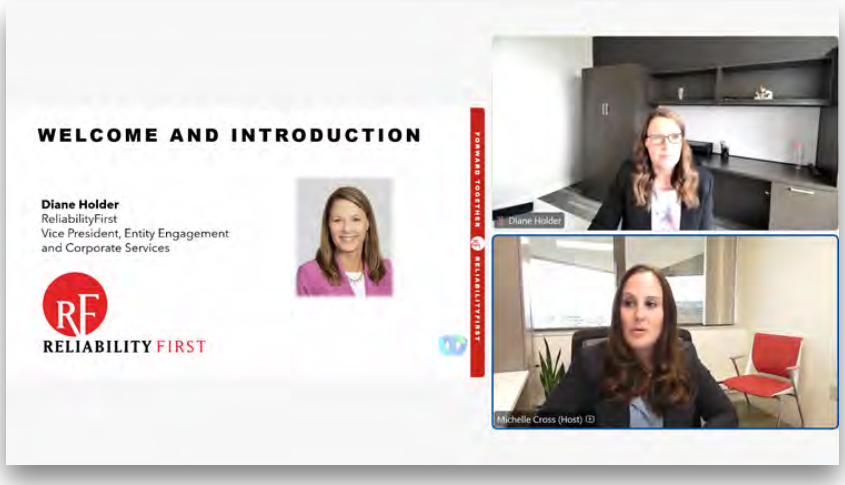
There was much discussion with the senators on cold weather preparedness, the potential gap between fossil fuel power plant retirements and renewable energy coming online, and the importance of essential reliability services (services that provide sufficient voltage, frequency support, and ramping capability to keep the electric grid in balance and stable).

Haque also discussed PJM's recently issued report, Energy Transitions: Resource Retirements, Replacements & Risks, which focuses on near term resource adequacy challenges and potential solutions. The public written testimony documents are linked here: RF testimony, PJM testimony, PA PUC testimony.

RF hosts first State Energy Policy Webinar

ReliabilityFirst hosted its first State Energy Policy Webinar on March 13, focusing on how states can ask the right questions to keep power reliable and secure for their citizens as the electric grid transforms. The event featured speakers from the Federal Energy Regulatory Commission (FERC), North American Electric Reliability Corporation (NERC), PJM, MISO and RF.

The event drew more than 460 total attendees, including representatives from 19 different states.



Stay tuned for launch of State Energy Policy Newsletter

In addition to webinars, RF is also launching a state energy policy newsletter this year. These initiatives are part of a push to establish RF as 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.

Tech Talk Recap

RF hosted three Tech Talks this quarter. Topics included:

- A discussion of the ReliabilityFirst 2023-2027 Strategic Plan and 2023 kickoff with RF Senior Vice President, Reliability and Risk, Jeff Craigo and RF Vice President, Entity Engagement and Corporate Services, Diane Holder
- A resource adequacy assessments summary from RF Principal Engineer, Engineering and System Performance, Tim Fryfogle
- A CIP themes roundtable discussion facilitated by RF Managing Enforcement Counsel Tom Scanlon, featuring panelists Lew Folkerth, Principal Reliability Consultant, External Affairs, RF; Tony Freeman, Principal Analyst, Risk Analysis & Mitigation, RF; Zack Brinkman, Manager, CIP Compliance Monitoring, RF; Robert Vaughn, CIP Auditor, SERC
- A presentation on upcoming changes to establishing and communicating System Operating Limits with Dean LaForest, Project 2015-09 Chair 2019-2021 and Manager of Real-Time Studies at ISO-NE, Vic Howell, Project 2015-09 Chair 2015-2019 and Director of Reliability Risk Management at WECC, and Stephen Whaite, Technical Auditor, Operations & Planning Compliance Monitoring, RF
- An update from the RF Operational Analysis and Awareness (OAA) team, featuring OAA Senior Manager Tony Purgar, OAA Principal Analyst Kellen Phillips and OAA Principal Analyst Dwayne Fewless

RF hosts first in-person Community Appraisal Event

RF piloted its community appraisal program with an in-person event in the city of Painesville, Ohio, on Feb. 7. The program focuses on improving a community's readiness, preparedness and resource strength for long-term disruptions to electrical grid-power and other community threats.

Representatives from the city, police, fire department, county emergency management agency, county board of commissioners, local utilities, county health district and city school district attended the Painesville event. They participated in an exercise designed to teach the players about ways their community can work to improve its resiliency in the event of a loss of grid power.

Calendar of Events

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

Date	RF Upcoming Events
4-17-23	Technical Talk
4-26-23	Q1/Q2 Board of Directors Committee Meetings
4-27-23	Q1/Q2 Board of Directors Meeting
5-15-23	Technical Talk
6-12-23	Technical Talk

Industry Events

Date	Industry Upcoming Events
4-20-23	FERC Open Meeting
5-1-23	PJM Annual Meeting
5-10-23	NERC Board of Trustees Meeting
5-18-23	FERC Open Meeting
6-13-23	MISO Board of Directors Meeting
6-15-23	FERC Open Meeting
6-20-23	FERC 2023 New England Winter Gas-Electric Forum
6-22-23	PJM Members Committee, Markets & Reliability Committee

ReliabilityFirst Members

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