Issue 3
2022 Q3

INSIDE THIS ISSUE

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

Follow us on:

RELIABILITY FIRST

Risk Based

Note from the President

Dear Stakeholders,

It was great to see some of you in person again at our annual Reliability and Compliance Workshop after hosting the event in a virtual-only format the past two years. If you came out to our offices here in Cleveland, thank you for making the trip and we hope you enjoyed the conference. And if you joined us virtually via Webex, I hope you enjoyed the presentations and I invite you to join us in-person next year when we head to Pittsburgh for our September 2023 Fall Workshop.

The central question I posed to our audience at the workshop was, what keeps me up at night? The answer is one you may have heard me give before: not knowing what I don't know. Our industry is facing all kinds of challenges at the moment, from increasing demand, to generation retirements, to dealing with extreme weather events at the same time that our dependence on weather-driven resources like solar and wind is also increasing. But what's coming next? One thing I've learned in this business is that there are always blind spots – acknowledging that they exist is the first step toward addressing them. I encourage you to expand your knowledge base – talk to people from different industries, countries and cultures. At this year's workshop we were fortunate to have presentations from Dragos CEO and Co-Founder Robert Lee as well as Micron Technology Vice President of Indirect Procurement Heather Baldwin. I hope you found value in their respective outside-of-industry perspectives on Operational Technology (OT) cyber threats and recommendations for the electric sector and the intersection between the supply chain and the manufacture of microchips and the electric industry.

This issue's theme is all about dealing with risk. In my view, the worst way to learn about a risk is by experiencing it. Being nimble, proactive and forward-looking is the best way we can be ready for these so-called "unknown unknowns." In "Continuous Improvement," we highlight RF's IRPAT tool, an exercise entities can use to improve their Incident Response Programs. In "The Lighthouse," we'll take a look toward the future of Critical Infrastructure Protection as it pertains to cloud-based technology for OT environments. And in "Enforcement Explained," we'll dig into how collaboration between the regulator and the regulated can help us be proactive in preventing potential harms to the grid.

When I was wrapping up my introduction at our workshop, I was also asked what helps me sleep at night – the answer is knowing that our industry is full of good people working to keep up with all of the challenges we're facing. It's up to all of you on the ground to identify the emerging risks you're seeing and to bring them to RF and NERC so we can all be ready when they occur. Together we can keep the grid reliable and secure.

Be safe and be well.

Forward Together,

Tim

From the Board

ReliabilityFirst (RF) held its Q2/Q3 Board of Directors Meeting on Aug. 25, 2022. RF President and CEO Tim Gallagher provided updates remotely, including his excitement at having Jenifer French, chair of the the Ohio PUC (PUCO), in attendance.

Mr. Gallagher highlighted items from the recent NERC Board Meetings in Vancouver, including FERC's approval of all 2023 business plans and budgets, work on an upcoming retrospective on the 20th anniversary of the blackout, and finally the robust discussion around resource adequacy and the future.

Then RF Board Chair Simon Whitelocke introduced Chair French, by sharing her background beginning with her public service on Westerville City Council, serving as a Common Pleas Judge in Franklin County and currently serving as the Chair of PUCO. Chair French noted she enjoys the impact she can have by serving all of Ohio and she covered the PUCO's role in electric reliability, gave an overview of their service monitoring and enforcement on the service quality side, and shared what her staff performs. A robust discussion with board members followed.

The 2022 Q4 ReliabilityFirst Annual Meeting of Members and Board of Directors and Committee Meetings will be held Dec. 7-8, 2022 in Arlington, Virginia.

Click here for more information and to register.

Continuous Improvement

By Sam Ciccone, Principal Reliability Consultant

How to use IRPAT to improve your Incident Response Program

The Journey to Security, Resiliency and Reliability

"Ask for help not because you're weak, but because you want to remain strong" – Les Brown

Tabletop exercises and incident response drills are being implemented throughout industry as a way to prepare and train operations and analysis personnel and emergency responders for the wide range of conditions they may face. We love seeing this because we believe it is a great way to preserve and enhance the reliability of the Bulk Power System (BPS). Did you know that RF can help you plan and execute these drills? RF offers the Incident Response Assessment Tool (IRPAT) that can help you test incident response and preparedness capabilities. Here we'll dive into the risks you can self-assess and help mitigate with IRPAT, as well as the benefits you could see on your continuous improvement journey.

How it works

The IRPAT tool provides users the opportunity to evaluate and benchmark their incident response and recovery posture, as well as measure effectiveness by performing simulated cyber or physical incident exercises. It can help characterize an entity's ability to gather and analyze threat intelligence and information from the affected systems and test incident response procedures as they relate to the entity's corporate, BPS, IT and OT environments. It has a repository of current threats with simple to advanced scenarios to test and measure historical performance. For a custom experience, entities can also use the customizable interface to craft relevant cyber and physical test scenarios and conduct tabletop exercises. If you already partake in GridEx, IRPAT can help build on that experience, which is only offered once a year.

The exercises are designed to expose participants to an array of realistic hypothetical scenarios. Here are some of the scenarios participants can explore within IRPAT:

- Denial of Service – Users with proper permissions become unable to access their required information due to cyberattacks. This simulation will present a hypothetical attack that could leave grid operators temporarily blind to generation sites by a cyber event that could potentially impact electric power system adequacy or reliability.
- Dragonfly 2.0 – The Dragonfly group appears to be interested in both learning how energy facilities operate and gaining access to operational systems themselves, to the extent that the group now potentially can sabotage or gain control of these systems should it decide to do so.[1]
- DYMALLOY – Uses common malicious behaviors like spear phishing campaigns to directly target individuals' digital communications and watering hole attacks that place malware on industrial-related websites to steal corporate credentials.[2]
- Other scenarios include ELECTRUM, Ransomware, SANDWORM and more.

What is IRPAT?

- Objectives:
  - Drive consistent, high-quality and realistic exercises
  - Continuously evaluate incident preparedness by utilizing an on-demand database of various cyber and physical security scenarios that go beyond GridEx
- Deliverables:
  - Lessons Learned reports
  - Best practices on incident response and preparedness
- Value add:
  - The ability to learn from a vast database of anonymized incidents

[1] Dragonfly: Western energy sector targeted by sophisticated attack group

[2] Dragos

Continued on page 4

Continuous Improvement

Continued from Page 3

IRPAT Benefits for Entities

- Helps demonstrate annual/periodic testing of incident response and preparedness procedures, as required by CIP-008-6, *(Cyber Security — Incident Reporting and Response Planning)*
- Benchmarks incident response posture and capability against other entities and previously conducted IRPAT assessments
- Offers anonymized lessons learned and best practices as a guide
- Grants access to contact resources for incident response handling (DHS, FBI, E-ISAC, local law enforcement)

Making IRPAT a part of your Continuous Improvement Journey

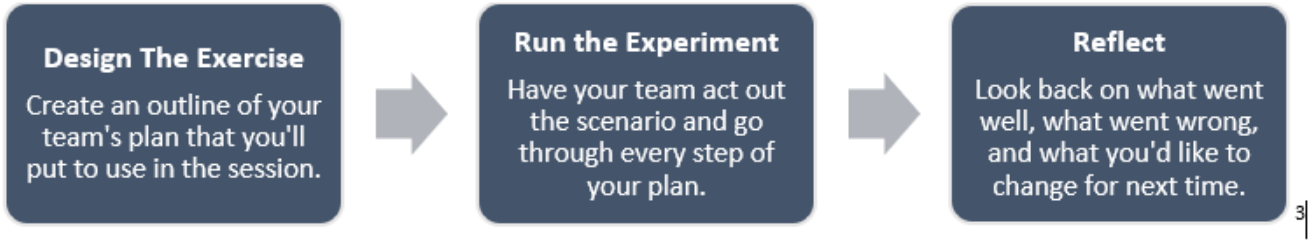
IRPAT and tabletop exercises are effective continuous improvement tools to achieve a resilient and mature incident response plan, and RF can help with training, set-up and facilitation of these assessments. For more information on the IRPAT tool and how to perform this free self-assessment, please contact RF's Entity Engagement department using the form on our website's Contact Us page.

At the end of the IRPAT assessment, the tool generates an extensive report that will provide BPS operators and personnel the ability to identify areas of improvement through deeper insights into components and processes that affect incident response and recovery. These "after action" reports help participants reflect on how the exercise went, documenting incident response areas to improve and initiating those improvement opportunities.

How to maximize IRPAT as a Continuous Improvement tool

Ensure participants are engaged and know their role. This includes the primary participants that are integral to the exercise: a facilitator who keeps the flow of conversation going while trying to get answers and ideas from the participants, an evaluator who identifies improvement opportunities and an observer.

And as you are used to hearing me discuss in this column, the overarching Deming Continuous Improvement Cycle "Plan Do Check Act" (PDCA) also correlates directly to the steps to create and perform a tabletop exercise, as shown below:



[3]

You can also find further information using these additional resources:

Incident Response Preparedness Assessment (RF IRPAT tool information on rfirst.org)

CIP-008-6 — Cyber Security — Incident Reporting and Response Planning

Incident Response Preparedness Assessment Tool (IRPAT)

Incident Response Preparedness Assessment Tool FAQ

GridEx VI - Lessons Learned Report, April 2022

NARUC – Cybersecurity Tabletop Exercise Guide

Crisis Management Tabletop Exercises – A Guide to Success

Do You Use Tabletop Exercises to Improve Performance?

5 Key Benefits from Conducting Tabletop Exercise

[3] How to Create and Run Tabletop Exercises

The Seam

By PJM Interconnection

PJM Monitoring Solar Storms for Geomagnetic Disturbances

A solar storm that may affect the earth's magnetic field is a fairly rare event, but one with potential impacts to the electrical grid.

PJM Interconnection, the country's largest grid serving 65 million people in 13 states and the District of Columbia, issued a warning Aug. 17 to its generation and transmission companies that a possible geomagnetic disturbance could impact the PJM system that evening. This came as PJM was monitoring for potential impacts of the solar storms that began Aug. 14.

The alert, issued for all of the PJM footprint, warned generation and transmission operators in case they would have to take prescribed steps in their operations to offset the impacts of such a phenomenon. No impacts to operations were reported during the warning period.

The last time PJM issued a warning to prepare for a potential geomagnetic disturbance was May 2021. As is most often the case, there was no reported effect on the PJM system at that time either.

What Is a Geomagnetic Disturbance?

Geomagnetic disturbances, which are also called solar magnetic disturbances, are caused by activity on the surface of the sun.

Sunspots, solar flares or other phenomena can produce large clouds of plasma, called coronal mass ejections. Should these super-charged solar winds come close enough to the Earth's magnetic field, they may induce electric currents within the ground and on high-voltage transmission lines. These currents can flow up from the earth or down into the earth through grounded grid equipment, usually transformers.

High levels of these unusual, volatile storm currents have the potential to damage transmission equipment.

For example, a major geomagnetic disturbance on March 13, 1989, caused a nine-hour power disruption in Quebec and also severely damaged a transformer at the Salem Nuclear Power Plant in Salem County, New Jersey.

The Space Weather Prediction Center of the National Oceanic and Atmospheric Administration (NOAA) monitors both solar activity and the earth's magnetic field. NOAA issues alerts and warnings to grid operators, so they can prepare for the impacts of space weather events.

The storm watch issued by NOAA on Aug. 17 prompted PJM's alert.

When solar storms brush against the earth's atmosphere, unusual sightings of the colorful northern lights' aurora may also be visible in the skies of southerly latitudes, including in the Mid-Atlantic and Northeast regions.

How Does PJM Protect Against Geomagnetic Disturbances?

When the NOAA Space Weather Prediction Center issues an alert to PJM rated above a certain threshold, PJM issues a warning to generation and transmission operators to prepare for potential disturbances.

To help anticipate problems, PJM's members have installed special equipment to detect and measure ground-induced currents caused by such geomagnetic disturbances. When a disturbance is forecasted, PJM monitors the installed detectors at various locations. If sustained ground currents at a certain level are detected, PJM operates the system in a more conservative mode until the space weather event has ended. The PJM Manual for Emergency Operations provides greater detail on the actions PJM and members take in response to a potential geomagnetic event.

Read more about geomagnetic storms and their impacts outside of the electricity industry on the NOAA website.

Enforcement Explained

By: Patrick O'Connor, Senior Counsel

Risk-based Regulation

Generally, risk-based regulation involves the regulator working collaboratively with the regulated organizations for the proactive prevention of harms. To accomplish this goal, the regulator must have a nimble, mission-driven approach to determine the issues it will focus on and utilize the appropriate mechanisms to influence behavior that will mitigate the potential harm posed by those issues. This process has been described as the "craft of regulation."

RF practices the craft of regulation in the enforcement context by utilizing mechanisms that are designed to enable RF and Registered Entities to focus their time and resources on issues that pose a higher risk to the bulk power system (BPS).

This approach raises two questions: (1) how does RF determine the potential risk posed by a potential noncompliance; and (2) how does RF resolve violations differently depending on their risk level?

Determining Potential Risk Posed by a Potential Noncompliance

Once a potential noncompliance has been identified (regardless of whether it was self-identified by a Registered Entity or identified by RF through a compliance monitoring engagement), the RF enforcement staff in conjunction with the Risk Analysis and Mitigation (RAM) department initiate the risk assessment process.

This process begins with building the factual record to ensure that RF has all of the information necessary to make a risk determination. Below are some examples of the types of information that we typically seek out at this step of the process:

1. A detailed explanation of how the Standard and Requirement were violated
2. An adequate explanation of the root cause
3. Start and end dates with adequate justifications
4. Information concerning extent of condition review
    a. The results of the review, if one was performed
    b. An explanation for why one is not necessary, if one was not performed
5. Other factors impacting the potential risk of the potential noncompliance (both mitigating and aggravating). Examples include:
    a. System conditions during the event
    b. Any internal controls in place that helped detect or correct the issue quickly
    c. Type/function of components or devices impacted
    d. Redundant or complementary internal controls in place to reduce the risk posed by the potential noncompliance

If there are any relevant facts that are unknown, RF enforcement will issue a request for information to the Registered Entity to obtain them. In addition to the factors mentioned above, RF also analyzes entity-specific considerations such as the entity's size, structure and location, and the maturity of the entity's preventative, detective and corrective controls.

Based on all of this input, RF makes a final determination of the risk posed by the potential noncompliance – i.e., minimal, moderate or serious.

Resolving Potential Noncompliances Differently Depending on Risk Level

After RF has made a final risk determination, the next step of the disposition process involves determining the appropriate disposition track for the potential noncompliance: Compliance Exception, Find Fix and Track (FFT) or Settlement Agreement. Each of these disposition tracks is tailored to a different risk level, with Compliance Exceptions and FFTs involving more streamlined processes that reduce the time and resources required to resolve.

Generally, minimal risk violations are disposed of via Compliance Exception, lower moderate risk violations are disposed of via FFT and higher moderate risk issues and serious risk issues are disposed of via Settlement Agreement. However, many more factors come into play in choosing the appropriate disposition track, which can alter that general approach. Notably, over the last 5 years, RF has disposed of approximately

Continued on page 7

Enforcement Explained

Continued from page 6

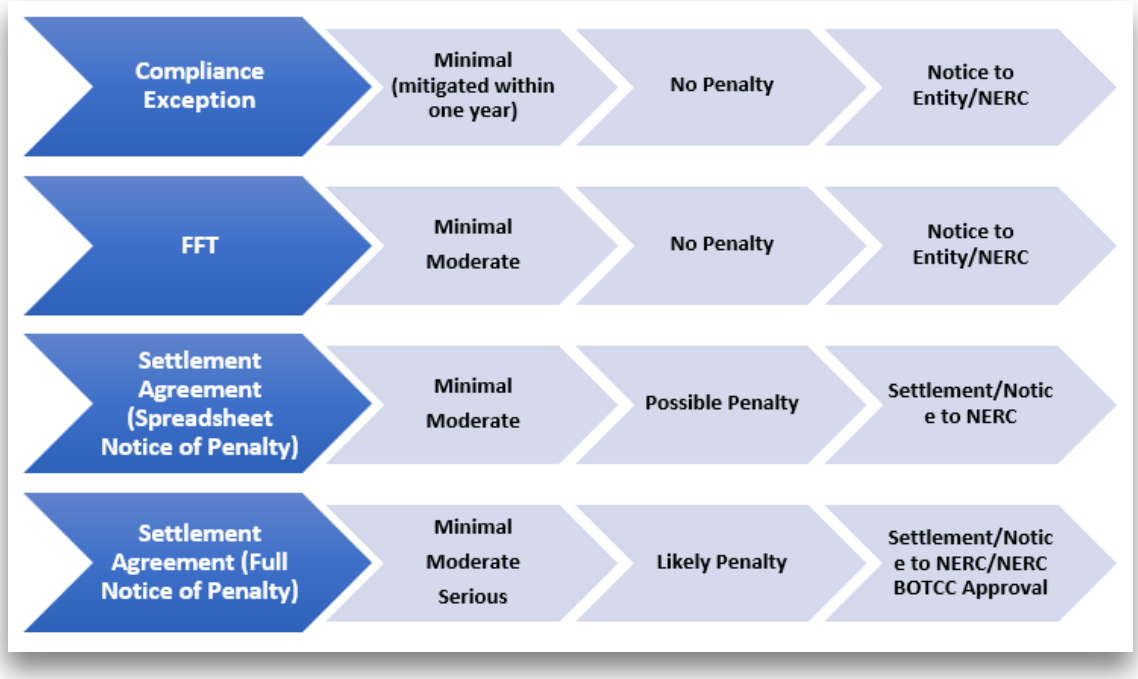
85% of potential noncompliances without a monetary penalty, meaning that the overwhelming majority of cases follow the Compliance Exception and FFT disposition tracks.

An entity's compliance history may aggravate the disposition track of a violation when it includes: (a) violations with the same root cause as the instant violation and mitigating actions that should have prevented the instant violation; or (b) programmatic failures involving the same or closely related Reliability Standards and Requirements.

Additional examples of other factors that may impact the disposition track of a violation include considerations such as how similar issues have been disposed of both within RF and throughout the ERO and whether a violation is part of a larger group of violations that arose from a common set of facts or demonstrate a common theme.

Considering how similar or comparable matters have been disposed of both within RF and throughout the ERO, while not binding, helps ensure that our outcomes are reasonable and that entities are not being treated unfairly. Moreover, sometimes one common set of facts gives rise to several violations with varying risk levels. In some of those cases, it is necessary to package those violations together in one disposition in order provide the full background and context of the violations, which helps facilitate a better understanding of the risk posed by all of the violations involved.

The graphic below is a quick guide to the distinctions between the different types of disposition methods:



Conclusion

Our goal in the enforcement department is to work collaboratively with our entities to ensure the proactive prevention of harms. To that end, if you have any questions on any of the information provided here, please reach out to your case manager who can discuss it with you in more detail.

The Lighthouse

By Lew Folkerth, Principal Reliability Consultant

CIP in the Cloud

This article is based on a presentation I gave at the 2022 NAES NERC Conference and the September Technical Talk with RF. It included additional background information about cloud services that you can read by viewing the presentation here.

In contacts with some of RF's Registered Entities, I'm seeing a movement of some operational functions to cloud-based technologies. A prime example is workflow management, where the software providers are well along in a Software as a Service (SaaS) delivery model. Some of these providers use methods that do not fit well with even the latest CIP Standards. Note that I am not necessarily promoting the use of cloud systems in the Operational Technology (OT) space, but I believe some cloud adoption is inevitable and we should get ahead of the adoption curve.

Potential Cloud Drivers for OT

Why move OT systems to the cloud? Unlike the move of IT systems into the cloud, moving OT systems should not be about cost. The only good reason to move OT systems to a cloud environment will be to improve reliability, resilience or security.

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.

Reliability consists of not letting problems happen. This is normally accomplished in OT systems by redundancy. Cloud environments can provide a large amount of redundancy, as this is their strength. Making use of a multi-cloud environment using more than one cloud service provider (CSP) in a failover situation may also help to achieve a highly reliable OT architecture.

Resilience means recovering swiftly and smoothly if problems do occur. Improved resilience might be achieved by leveraging some of the features of cloud computing such as geographic diversity. This can prevent a widespread event (hurricane, wildfire, flooding, etc.) from affecting all of your OT resources. Another cloud benefit is elasticity, where resources available to a service can dynamically expand when needed.

Grand Haven, MI – Photo: Lew Folkerth

Security includes assuring availability, integrity and confidentiality. Moving to a cloud environment can improve security in some areas, but can also pose challenges in other areas. The CSP provides security for the physical facilities, servers and networks. Depending on the service model (see background information referenced above), the CSP may also provide security for the operating system and the application software.

Elasticity is a property of cloud computing that permits dynamically expanding the resources available to a process or service. When computationally intense processes are used in real-time or near-real-time environments, these processes may be able to benefit from the effectively unlimited computational resources available in the cloud.

Operational Challenges for OT Cloud Services

In counterbalance to the benefits above, any move of OT services to cloud providers will present significant operational challenges. I've listed some of those challenges below.

Availability is a measure of the "uptime" of a system, usually measured as a percentage. Major CSPs quote various levels of availability depending on services, some levels as high as 99.99% (four nines, or 52 minutes of downtime per year) availability. However, SCADA systems target a higher availability, usually 99.999% (five nines, or five minutes of downtime per year). In addition to

Continued on page 9

Continued from page 8

system availability, network and storage availability will also be critical factors.

Latency is a measure of the delay from data generation to data consumption. Major CSPs use the public Internet for communications, so there is the possibility of delay and dropped communications between the data endpoints.

Mobile access is the ability to easily access cloud services from any device anywhere in the world. While this feature can be a huge benefit for IT systems, it can present serious problems for OT. We do not want anyone, anywhere, to be able to control the breakers in a substation or the feed pump in a steam generator.

Financial challenges include not just the cost of cloud services, but the type of money used. For some utilities, on-premises computer systems are capitalized and can be added to the utility's rate base. Cloud services will use operational dollars.

Cyber security tools and processes will be different in a cloud environment. Entities using cloud services for operational systems will need to train personnel and adapt processes and tools to the new environment.

Compliance Challenges for OT Cloud Services

The use of cloud services will not be possible under the present CIP Standards except in the most limited case, such as some forms of BES Cyber System Information (BCSI) in the cloud. New Reliability Standards will be required, and those Standards will need to be risk-based. There are too many variables in cloud environments to be able to write prescriptive Standards for these cases.

Compliance processes will need to be very mature and integrated with operational processes and procedures. Internal controls will become even more important.

Auditing processes will need to be adapted to cloud environments to determine the type, quality and quantity of evidence that will be needed to provide reasonable assurance of compliance.

Path Forward

To adequately prepare for the adoption of cloud services, I believe we need to develop use cases for this technology. We can then address the operational, security and compliance challenges for each use case. We should begin with known needs, such as cloud-based service providers (such as work management systems) that store BCSI in the cloud. After we take these initial steps, we can evaluate additional use cases.

We will need an environment in which we can test these concepts without incurring compliance risk to the Responsible Entities involved in this forward-looking work. There is precedent for this in the CIP version 5 Transition Advisory Group (v5TAG). The v5TAG provided a forum where transition from the version 3 CIP Standards to version 5 could be tested and modified as needed without incurring compliance risk. I suggest that a Cloud Technology Advisory Group (CTAG) be formed to experiment with and monitor the transition to cloud technologies.

If a CTAG is formed, it should be a partnership with ERO Enterprise staff and a small group of Responsible Entities that are interested in pioneering cloud technologies. Cloud services can be tested, and operational and security issues addressed. Potential revisions or additions to Reliability Standards can be outlined and compliance processes and evidence tested for effectiveness. In this way, cloud transitions can be performed in a small, controlled environment before right-sizing the use of cloud services.

Conclusions

I am not advocating the migration of OT systems and services to the cloud, but I believe some movement in this direction is inevitable.

Reduced cost, the primary driver of early cloud adoption, should not be a significant driver for real-time cloud migration. Rather, the leveraging of cloud technologies for improved reliability, resilience and security should be the drivers, but the associated risks must be effectively managed.

The CIP Standards will need to be modified or new Standards developed to address cloud risks. These Standards will need to be explicitly risk-based to effectively adapt to the wide range of cloud service provider options and features.

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.

NERC Launches Reliability Vignettes

NERC is launching a new product called Reliability Vignettes, which are intended to capture current operating incidents of interest and project the circumstances of the incidents into the future as think pieces for system planning and operating considerations. NERC will publish Reliability Vignettes on an occasional basis as interesting system occurrences are identified.

The first Reliability Vignette — ***Future Wind Planning Informed by Current Operating Experience*** — uses the real-world operating experiences of two Balancing Authorities in a high-wind event as the basis for consideration of a future system that is wind- and solar-generation dominant. This document's objective is to provide future resource planning considerations for registered entities to consider and/or implement as they design future operations of their system assets. Operating scenarios for the vignettes are summarized in an unattributable manner and shared with the industry, policymakers and interested parties.

Reliability Vignettes will be available on the **Event Analysis, Reliability Assessment, and Performance Analysis** page of NERC's website.

Regulatory Affairs

Department of Energy Issues Request for Information on Grid Initiatives

The Department of Energy (DOE) has issued a request for information (RFI) to help finalize its five-year, $10.5 billion program under the Infrastructure Investment and Jobs Act to revamp the nation's power grid and increase resiliency. The RFI seeks public input to help inform DOE's implementation of the law.

The funding will be split into three initiatives: $2.5 billion in grid resilience grants to reduce the impact of extreme weather and natural disasters, $3 billion in "smart grid" grants to increase flexibility and reliability of the power system, and $5 billion to give states financial assistance to innovate transmission, storage and distribution infrastructure. This funding will be administered through the DOE's Grid Deployment Office.

National Security Telecommunications Advisory Committee Releases Report on Risks Related to Information Technology

The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) issued a draft report that warns of cybersecurity vulnerabilities. The report was prepared by the President's National Security Telecommunications Advisory Committee (NSTAC), which was asked to focus on key cybersecurity issues related to national security and emergency preparedness.

The report focuses on the risks arising from the convergence of IT and Operational Technology (OT) systems. When IT and OT systems converge, formerly standalone OT systems like electrical substations are connected to the internet, which then introduces risks to the OT system.

The report flags commonly seen issues that can allow cyber attackers to move into an entity's OT network from its IT network. First, many entities create an "air gap" that isolates IT and OT systems from each other, but these air gaps often break down and become ineffective for various reasons described in the report. Second, there can be "accidental convergence" of the IT and OT systems, which happens when the system owner doesn't know or can't see where devices are in their networks. Additionally, there can be "shadow IT," where OT systems are added and modified without getting official IT change management and approval.

The report also includes recommendations on how to address these risks, such as breaking down silos between IT and OT teams and prioritizing resources to ensure the cybersecurity of OT systems.

FERC Issues Notice of Proposed Rulemaking on Cybersecurity Incentives

On Sept. 22, 2022, FERC issued a Notice of Proposed Rulemaking on Cybersecurity Incentives (NOPR) to establish rules providing incentive-based rate treatment for utilities that make certain cybersecurity investments to help safeguard against and respond to cyber threats and for utilities that participate in cyber threat information sharing programs.

To qualify for the incentives, cybersecurity investments or information sharing would have to materially improve the utility's cybersecurity posture and not already be required by the CIP Standards or other laws. In the NOPR, FERC proposes to establish a pre-qualified list of cybersecurity investments that are eligible for incentives, and this list would be maintained on the FERC website. Approved incentives would remain in effect for up to five years.

The incentive-based rate treatment for entities making these investments would take two forms: either a return on equity adder of 200 basis points, or deferred cost recovery that would enable the utility to defer expenses and include the unamortized portion in its rate base. Additionally, entities that receive an incentive would have to make an annual informational filing that discusses the cybersecurity investments they made.

The NOPR will be open for a 30-day comment period.

Standards Update

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

General NERC Standards News

Extreme Cold Weather Grid Operations, Preparedness and Coordination Group Provides Technical Reference

In August of 2022, the 2021-07 standard drafting team developed and posted a technical reference document for calculating extreme cold weather temperature. The intention is for this document to walk through one method for acquiring the necessary weather data for a location and then use that information to perform statistical analysis to determine the Extreme Cold Weather Temperature for the location.

ERO Enterprise Updates CIP-012-1 FAQ

Based on a June 2, 2022 roundtable discussion, the ERO Enterprise recorded questions and responses on CIP-012-1, then those items were memorialized and added to the CIP CMEP FAQs document.

Notable NERC Filings

In July-September, NERC filed the following with FERC:

- On Aug. 17, 2022, NERC and the Regional Entities (ERO Enterprise) submitted comments on a FERC Notice of Proposed Rulemaking (NOPR) regarding proposed changes to FERC's existing regional transmission planning and cost allocation requirements. For reasons discussed therein, the ERO Enterprise's comments are filed in support of FERC's NOPR.
- On Aug. 30, 2022, the ERO Enterprise submitted comments on a FERC NOPR regarding Extreme Weather Vulnerability Assessments. In the filing, the ERO Enterprise supports FERC's proposal to direct submission of one-time information filings regarding current or planned processes for conducting extreme weather vulnerability assessments.

Notable FERC Orders

In July-September, FERC filed the following:

- On July 28, 2022, FERC filed a NOPR seeking comment on the implementation of a "Duty of Candor" standard for communications with the Commission.
- On Aug. 25, 2022, FERC issued an order approving revisions to the NERC Rules of Procedure regarding Reliability Standards. The order in part finds that "[t]he modifications will allow NERC to remove duplicative language in the Rules of Procedure, eliminate dated provisions, and provide more clarity and flexibility with respect to RBB [Registered Ballot Body] participation and the segment criteria review."

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	
Oct. 1, 2022	CIP-005-7 -- Cyber Security -- Electronic Security Perimeter(s); CIP-010-4 – Cyber Security – Configuration Change Management and Vulnerability Assessments; CIP-013-2 – Cyber Security – Supply Chain Risk Management; PRC-024-3 – Frequency and Voltage Protection Settings for Generating Resources
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

Fall Workshop Recap

ReliabilityFirst hosted its 18th annual Compliance and Reliability Workshop Sept. 27-28 at the RF offices in Cleveland, Ohio. This was the first time RF hosted the workshop in person since October 2019, due to the COVID-19 pandemic, and many guests were excited to have the opportunity to be back interacting with their industry peers. The hybrid event drew 100 in-person guests and more than 300 attendees virtually through Webex.

The workshop included speakers from FERC, NERC, Dragos, Inc., E-ISAC, Micron Technology, Inc., ITC Holdings Corp. and RF. Additional special thanks to Dragos CEO and Co-Founder Robert Lee and Heather Baldwin, Vice President of Indirect Procurement at Micron Technology, for adding to a great workshop experience for our attendees by sharing their perspectives from outside the electric industry.

Between the two-day workshop, attendees heard a line-up of presentations on the transformation facing the electric industry; energy availability and the changing generation resource mix; OT cyber threats and recommendations for the electric sector; the electricity threat landscape and how that relates to the CIP-008 Standard; updates to the compliance monitoring engagement timeline for entities; the intersection between the supply chain and the manufacture of microchips and the electric industry; examples of compliance excellence; RF's state outreach efforts; integrating cyber and physical security concepts into transmission planning; the FERC internal network security monitoring NOPR; and an overview of the resources RF offers to help entities with reliability and security.

Watt's Up at RF

Outreach Recap

ReliabilityFirst (RF) is committed to providing timely and pertinent information to our entities and stakeholders. Our monthly open webinars provide a forum to address topics and questions relevant to reliability, resilience and security. During our Technical Talks with RF, we host a range of speakers and subject matter experts across the industry. The Technical Talks with RF are typically the third Monday of each month (but may be moved to avoid holidays). Our calendar of upcoming events, with agendas and the Webex link to join, can be found on our website, rfirst.org.

Some of the speakers so far this year have included:

- **Tim Fryfogle, RF Principal Engineer - Resources**, presented on the winter recap of GADS data, forced outages, lessons learned and opportunities for improvement within RF's footprint.
- **Tim Kucey, PSEG Manager NERC Standards & Advocacy**, showcased how PSEG prepares for winter and their implementation of recent FERC/ERO recommendations to enhance reliability.
- **Clarice Zellmer, WE Energies Engineering Manager**, showcased how the WEC Energy Group prepares for extreme weather and their implementation of recent FERC/ERO recommendations to enhance reliability.
- **Derek Kassimer, RF Principal Technical Analyst**, provided an overview of RF's winterization efforts, including our annual survey, winterization visits and ERO resources available.
- **Nick Poluch, Talen Energy Senior NERC Manager, and Colleen Dolan, Talen Energy NERC Internal Controls Manager**, co-presented on Talen Energy's journey with their internal controls program and implementation.
- **V. Jason Smith, DTE Energy Director NERC Compliance, Anna Pawlak, DTE Energy Supervisor NERC Security and Compliance, Patrick Elliott, DTE Energy Senior Auditor NERC Compliance, and Jeff Wallace, DTE Energy Specialist NERC Compliance Process Management,** co-presented on their internal controls journey and their upstream focus on preventing and mitigating risks.
- **Tony Jablonski, RF Manager, Risk Analysis & Mitigation**, provided an update on the Align tool.
- **Lew Folkerth, RF Principal Reliability Consultant**, presented on cloud technologies, the benefits to reliability and incorporating into a compliance framework.

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

Protection System and Human Performance Workshop Recap

RF hosted its 8th Annual Protection System Workshop on Aug. 3 and the 5th Annual Human Performance (HP) Workshop on Aug. 4. The Protection System Workshop had more than 170 participants and the Human Performance workshop had over 150 participants.

Both workshops were organized and coordinated by the Engineering & System Performance department. Although the event was hybrid (i.e., both in-person and virtual), the events provided an opportunity for Registered Entity personnel to interact with their counterparts by asking questions, learning new techniques and procedures and sharing their real-life experiences.

Protection System Highlights

The focus for the Protection System Workshop this year was on activities related to incorporating Inverter Based Resources (IBR) into current planning and design processes. The workshop featured presentations on the latest Protection System Misoperation trends across RF and the NERC footprint; implementing protection systems while dealing with IBR challenges; the IEEE 2800 standard and the motivation for its development; PPLEU's implementation of Dynamic Line Ratings and the impacts to protection system design; AES Ohio's plan to address FERC Order 881 and an overview of their FAC-008 program; and an overview of the Microprocessor Relay Failure Mode & Mechanism Diagram being developed by the NERC Failure Modes and Mechanisms Task Force.

Human Performance Highlights

The focus for this year's Human Performance event was the use of a variety of approaches to reduce human error in dynamic environments. Workshop presentations included a review of statistics on facility outages caused by human error; an overview of and background for the development of the Canadian Standard, psychological health and safety in the workplace; practical ways to build psychological safety in high hazard industries; emerging cyber threats to the Bulk Electric System and the IEEE-NERC Security integration Project; real-world experiences where maintenance processes and system design can have problems when human performance is not taken into consideration; and a review of the NERC event analysis process, the development of lessons learned and an in-depth review of two events caused by human performance issues.

Upcoming October Technical Talk with RF

Join us for our upcoming Technical Talk with RF on Monday, Oct. 24, 2-3:30 p.m. The presentations will include an update on recent reliability related activity from Kal Ayoub, FERC Deputy Director, Division of Cyber Security, and Andrew Bochman, Idaho National Laboratory Senior Grid Strategist, speaking on advanced small nuclear reactors.

Watt's Up at RF

Day of Giving Recap

City Mission

Providence House

Arkansas Food Bank

ReliabilityFirst employees spent the morning of Sept. 13 giving back at four Cleveland organizations: Cleveland Metroparks, the Avon Hunger Center, Providence House and the City Mission.

And three of our teleworkers based in Arkansas also got together to volunteer at the Arkansas Food Bank.

Cleveland Metroparks

Avon Hunger Center

RF Gives back

Calendar of Events

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

Date	RF Upcoming Events
Oct. 24	Technical Talk with RF
Nov. 14	Technical Talk with RF
Dec. 7-8	Annual Meeting of Members and Q4 Board of Directors and Committee Meetings
Dec. 12	Technical Talk with RF

Industry Events

Date	Industry Upcoming Events
Oct. 6	FERC Technical Conference on Transmission Planning and Cost Management
Oct. 12	PJM Electric Gas Coordination Senior Task Force
Oct. 20	MISO Winter Readiness Workshop
Oct. 24-26	PJM Markets & Reliability Committee, General Session, Members Committee
Nov. 2-3	NERC-NATF-EPRI Annual Transmission Planning and Modeling Workshop
Nov. 10	FERC Annual Commissioner Led Reliability Technical Conference
Nov. 14	Organization of MISO States Board Meeting
Nov. 14-16	NERC Board of Trustees Meetings
Nov. 15	Fifth Meeting of the Joint Federal-State Task Force on Electric Transmission
Nov. 16	PJM Members Committee
Nov. 21	PJM Electric Gas Coordination Senior Task Force
Dec. 5-8	MISO Board of Directors Meetings

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