Issue 5
2020 September/October

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:

Note from the President

Dear Stakeholders,

I've touched on the topic of balance a few times already this year. Our industry has done an outstanding job balancing pandemic response activities with normal, day-to-day work. RF leadership has aimed to strike a balance between implementing and communicating our pandemic response plans as quickly as possible while still remaining agile. Balance between our work and personal lives positively contributes to our overall well-being, which cannot be overstated during such a trying year.

Another message of balance that will remain important for the foreseeable future is the ever-evolving relationship between compliance and excellence. Compliance with Reliability Standards will always be fundamental to our industry, and the merits of continuous improvement efforts are well established beyond the electric industry. It's the intersection of these two equally-important objectives where I believe the most opportunities lie for mitigating risk in the face of new and emerging threats.

Bringing together compliance personnel and subject matter experts (SMEs) has become a bit of a passion for us at RF. Acting as an indispensable resource by sharing relevant information with the right people is a vital component of our efforts to strengthen the connection between compliance and excellence/continuous improvement.

We know one side of the equation cannot thrive without strong relationships, information sharing and open communication with the other – so it gives me great satisfaction to see more SMEs, in areas like cyber and physical security, operations, planning, design and others, joining our usual compliance contacts to participate in our outreach activities.

We pride ourselves on offering expertise and assistance to our entities, stakeholders and the ERO Enterprise as whole, so please take advantage of the value RF SMEs can add to these efforts at your own organization. If you missed any of our recent educational opportunities, such as the Insider Threats webinar or the presentation on cold weather readiness from the October Technical Talk with RF, please read the webinar and workshop recaps in this issue and visit RFirst.org for presentation materials.

Be safe and be well.

Forward Together,

Tim

From the Board

This year, RF was pleased to welcome two new members to the Board of Directors: Ben Felton and Joe Trentacosta. In this newsletter, we have asked Ben Felton, Senior VP of Fossil Generation at DTE Energy, to share some of his experience and thoughts for the term.

Please tell us a little about your educational background and professional experience.

After earning my bachelor's degree and MBA from the Gainey School of Business at Spring Arbor University (Spring Arbor, MI), I started my career at Consumers Energy in 1992. I held various positions throughout the company and worked my way up through gas, electric, supply chain, electric distribution, operations and maintenance. Prior to leaving Consumers, I was the Executive Director of System Operations and Maintenance, where I held responsibilities for distribution and high voltage distribution lines and subs, in addition to field technical services.

In 2015, I started as VP of Power Delivery with Northern Indiana Public Service Company (NIPSCO) out of Merrillville, IN, where I was responsible for transmission & distribution, metering, scheduling, budget and forestry. After two years, I moved into the role of Senior VP of Electric Operations, which encompassed my previous responsibilities plus generation, fleet, warehouse, safety and training for the entire company.

Currently, I am Senior VP of DTE's Fossil Generation, where I hold responsibilities for the company's fossil generation fleet, generation optimization, merchant operations and the enterprise's NERC compliance office.

What sparked your interest in joining the RF Board?

Over the past 15 years, I have worked closely with internal partners to assure that our program focus was solid and that we maintained excellent relationships with our regulators. Upon joining DTE in 2019, I was offered an opportunity to replace Matt Paul, who is now DTE's President and COO of gas, as the senior NERC manager. I jumped at the chance to get involved directly with RF and further my participation and education of the elaborate network of committed individuals who assure we have a safe and stable power grid.

How do you anticipate your experience will contribute to serving RF's entities and stakeholders?

I am hopeful that my extensive utility operations experience will enable me to fully participate with the broader team to define and advance the most sustainable compliance solutions that drive well aligned success.

Having prior experience at three different utilities also affords me a unique sampling of the grass roots perspective to driving a culture of security within the utility. Ultimately, I envision success as system owners and operators partnering with their respective regulators to further build a nimble system to protect our systems. Although my time at DTE is just over one year, I am excited to fully engage with a peer set I have built over 28 years to look for meaningful opportunities to learn, grow and improve with a mind-set of "as we grow together, we win together," which obviously is the goal nationwide.

What do you think the priorities for the industry should be in the coming years?

Being in Michigan, we lived through the automotive industry downturn in 2008-2009, and we saw what happened in our state. It was around that time that Amazon came on the scene where you could buy just about anything, and that really disrupted an entire industry. It's not implausible that they could be a direct competitor in the future, and that's really shifted my focus. Part of that focus is on what I can do as a leader, especially a leader over an electric operation, to guide my team to look for ways to create value for our customers. I want our customers to know that for every dollar they send us, there's a value that comes with it, so if they ever have a choice they will choose us over the next best option.

What is happening in the industry today that you are most excited about?

What I see across the industry is the transition away from coal plants – and, in the longer term, from all fossil fuels. Many of those plants, however, still will be critically important to system stability and providing reliable energy as we swiftly move through this transformation. So, I see the big challenge as how to run them to their retirement dates while keeping our teams engaged and connected to our purpose, all the while giving the same level of energy today as they did yesterday, and do that in a very safe and productive manner.

Thoughts from RF's New GC Niki Schaefer

2020 has certainly been a year of change, some expected and some not. Our Vice President and General Counsel, Niki Schaefer, began her new role in April when our office was closed and Ohio was essentially shut down due to COVID-19.

She offers some reflections on her experience at RF to date, what her professional background can add to the RF mission, and her vision for the future of the Legal, Enforcement, and Compliance Monitoring Teams she oversees.

What was it like to start a new role during a pandemic?

It was definitely strange, but I was happily returning to a company where I had already worked (as Managing Enforcement Counsel) and knew many of the people, and had a built-in understanding of and appreciation for the regulatory framework in which RF operates and its mission and values.

Given that I was stuck at home, I had some time to individually call many members of my team that I didn't already know to try and get to know them. I also had time to reconnect with old colleagues.

Everyone was incredibly helpful in bringing me up to speed on what I had missed in the ERO during the five years I worked for Eaton Corporation: process and organizational improvements, and the transformation effort undertaken by the regions and NERC and the risk-based, collaborative approach to which the ERO has committed.

I was blown away by all of the positive changes that were implemented in the time I was gone, yet still welcomed by the warm, inviting nature of RF that I remembered so fondly and to which I was looking forward to returning.

What unique perspective do you bring to your new role?

Prior to working at RF the first time as Managing Enforcement Counsel, I was a trial attorney litigating commercial, personal injury, and product liability cases across the country. Every new case required me to learn the subject matter of whatever business or product we were disputing, and learn that subject matter in such great detail that I could explain it to a jury clearly.

My key takeaways from that experience that apply to RF were that everything is learnable (which is good because there's lots to learn!) and the importance of being able to clearly and convincingly tell a story.

When I left RF to join Eaton, I held a variety of roles, but the most relevant involved serving as legal counsel to senior leadership teams across multiple business units within Eaton's Electrical Sector supporting more than $2 billion in revenue. In this role, I supervised litigation of all types and provided guidance on all areas of the law, including commercial contracts, NERC, regulatory and other compliance, product performance, cyber security, competition and trade, employment issues, and board and audit reporting.

There were so many parallels to my current GC role, but the most unique learnings and perspectives I bring from the role is that Eaton Corporation sells electrical products to many Registered Entities across the country, so that job required me to understand the commercial and operational impact of what RF does in a way I never would have appreciated.

What is your vision for your team and ReliabilityFirst as a whole?

Even though I oversee our compliance monitoring auditors and our legal and enforcement attorneys, two roles that can be viewed as almost adversarial, I see us as partners in reliability, security and resilience. We are partners within the broader RF organization, with other Regions, with NERC and FERC, and with our Registered Entities.

In order to be a valued partner in that effort, we need to listen and adapt to what we are hearing, be transparent about what we are doing and why, be thoughtful and risk-based in our decision-making, and collaborate with our ERO and stakeholder partners.

So much of the groundwork for all of this has already been laid, and I'm so excited to have such a great foundation upon which to continue building!

Continuous Improvement - Incident Management

By Sam Ciccone, Principal Reliability Consultant

The Journey to Security, Resiliency and Reliability

"Houston, we have a problem" – Apollo 13

Lew's Lighthouse article this month discusses Incident Management (IM) and response and the CIP-008[1] NERC standard. This standard's purpose is "To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements." It requires having and implementing an Incident Response Plan.

Incidents on the grid are inevitable. They can be caused by weather, bad actors, human error and equipment error, just to name a few. The key is: How resilient can you be to minimize the damage and get the grid running as normal?

The life cycle of an incident starts prior to event detection (e.g., building resiliency capabilities) and ends in analysis and response. But how do you improve that cycle from start to finish, and how do you improve your IM program? That depends on whether there are incremental changes needed due to incidents that have been known to happen, or are you in crisis mode due to a novel incident that requires significant improvements or even organizational changes? People make improvements happen, leadership empowers people to make the changes, and information and measurement keep the improvement efforts moving.

Continuous Improvement Suggestions and Methods

Your IM program should include the closure of incidents after your organization concludes remediation and the capture of lessons learned from incidents. Lessons learned are particularly important because they can inform your organization on where it can be more proactive to prevent incidents, rather than discovering them after they occur.

Learning from an incident and gleaning valuable information includes involving relevant stakeholders and translating a lesson learned into an action plan for the future. Your organization can utilize these lessons to inform its going-forward strategy, incorporating the lessons into overall grid reliability improvement. And, don't forget scenario brainstorming to consider incidents that haven't been experienced yet, instead of waiting until an incident occurs to learn and prepare.

Capability Maturity Models, Kaizen and Facilitation

Per the "CERT Resilience Management Model (CERT-RMM): A Maturity Model for Managing Operational Resilience,"[2] the purpose of Incident Management (IM) is: "To establish processes to identify and analyze events, detect incidents, and determine appropriate organizational response."

What are the feeders into IM (see Fig. 1)? CERT RMM discusses the relationships and practices that drive IM. The quality and maturity of these practices plays a direct role in IM and should be evaluated and continuously improved. I encourage you to read more about IM and these process areas in CERT RMM.

The diagram includes External Interdependencies (EXID). EXID play a role in IM, and this is a feeder where many risks to the electrical grid reside. One example risk in EXID is communications. This risk

Figure 1: Feeders into Incident Management

often involves internal, cross-departmental communication, as well as with external entities so that they take action or for general situational awareness. These communications should be anticipated whenever possible and documented in an IM plan. Required communications may span a long list of stakeholders, such as asset owners, IT staff, OEMs, supervisory staff, human resources, regulatory agencies, etc. These external groups may also be able to provide additional perspective not yet considered.

[1] https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-008-6.pdf

[2] https://www.amazon.com/Resilience-Management-Model-CERT-RMM-paperback/dp/0134545060/ref=sr_1_1?dchild=1&keywords=cert+rmm&qid=1602593262&sr=8-1

Continued on page 5

Continuous Improvement - Incident Management

Continued from page 4

What if you discover after tests, exercises, or actual incidents that your IM process is not effective?

One method of improvement for incidents that have occurred is a Kaizen event to facilitate any needed improvements. Kaizen involves cross-functional brainstorming focused on which of the IM feeders need to be improved. For example, you may find that you need additional resources and technology to improve Monitoring, which will drive more effective mitigation of incidents. For a more effective Kaizen, using an impartial facilitator, or even starting an internal program to develop your own "home grown" facilitators, brings objectivity to the discussion. A good source for planning and executing Kaizen events is "Kaizen Event Fieldbook: Foundation, Framework, and Standard Work for Effective Events,"[3] and a good source for Facilitation is "The IAF Handbook of Group Facilitation: Best Practices from the Leading Organization in Facilitation."[4]

How can we better prepare for incidents we've never seen before?

In the Apollo 13 quote at the beginning of the article, the U.S. space program had never seen such an issue before. Were they lucky they got through it? Or did they prepare for these unknowns? There were seasoned personnel on the ground and in the air, with competencies to react to incidents they never dealt with before. Their high level of competencies allowed them to keep the command module intact, and lives were saved.

For incidents never before seen, building personnel competencies (shown in Fig. 2) is imperative. In the book, "Managing Crises: Responses to Large-Scale Emergencies,"[5] two types of emergencies are discussed: routine and novel. According to the book, crisis (incident) management must be accomplished in novel emergencies. They further detail the competencies necessary for managing novel events and the differences between the competencies and characteristics necessary for routine emergencies. I will delve deeper into Competency Roadmaps in future articles.

So how do the feeders, known events, and never-before-seen events fit into the IM improvement process? Figure 2 depicts this process.

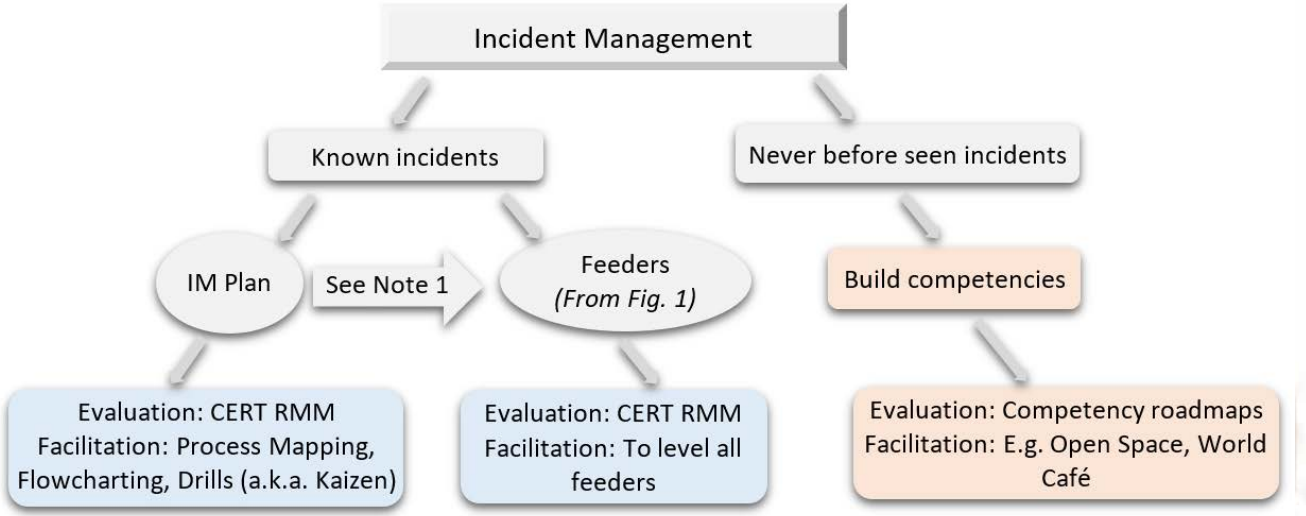
Conclusion

Effective Incident Management is vital to the electric utility industry, especially in today's environment with bad actors trying to hack our cyber systems[6] and those forces physically damaging critical operational assets (weather, foul play.) The methods and information provided here will hopefully give you some tools to improve your IM program.

If you need help facilitating a Kaizen event, creating a Competency Roadmap, or undergoing an Evaluation, please let RF know! You can submit an Assist Visit request to the Entity Engagement team, or you can contact Brian Thiry, Manager, Entity Engagement.

Figure 2: IM Categories and Improvement Activities

Note 1: Target enough feeders that help balance the inputs to the feeders into Incident Management



[3] https://www.amazon.com/Kaizen-Event-Fieldbook-Foundation-Framework/dp/0872638634/ref=sr_1_1?dchild=1&keywords=Kaizen+Event+Fieldbook&qid=1602593068&sr=8-1

[4] https://www.amazon.com/IAF-Handbook-Group-Facilitation-Organization/dp/078797160X/ref=sr_1_2?dchild=1&keywords=the+IAF+Handbook+of+Group+Facilitation&qid=1602593152&sr=8-2

[5] https://www.amazon.com/Managing-Crises-Responses-Large-Scale-Emergencies/dp/087289570X

[6] Related reference: RF's Insider Threat presentation from September 2020: https://rfirst.org/KnowledgeCenter/Workshops/KC%20%20Workshops%20Library/2020%2009-30%20Insider%20Threats%20Webinar%20Presentations.pdf

The Seam

By Midcontinent Independent System Operator, Inc. (MISO)

MISO Responds to Devastation of Hurricane Laura

What was the reliability impact of Hurricane Laura?

On August 27, Hurricane Laura made landfall as the strongest storm to hit Louisiana in more than 150 years, leaving 730,000 customers without power in Arkansas, Louisiana, Mississippi and Texas. The Southeastern Texas and Southwestern Louisiana areas of the MISO footprint sustained substantial damage to the transmission facilities under MISO's functional control and to interconnected generation and distribution facilities, requiring careful and deliberate focus on maintaining system stability.

How does Hurricane Laura compare to other hurricanes?

This is the first major hurricane event that MISO has been directly involved with.

According to Entergy, the damage caused by Hurricane Laura is some of the most severe they have ever experienced, surpassing that of Hurricane Gustav that hit Louisiana and Hurricane Ike that hit Texas in 2008. Hurricane Laura's historic intensity caused severe damage to the Entergy distribution and transmission systems on the chart.

What is the approach to making repairs?

Transmission lines that incurred major damage may need to be fully reconstructed in parts. A transmission structure that supports a 500,000-volt line weighs roughly 40,000 pounds. Transporting just one requires three 18-wheeler trucks. For comparison, one 18-wheeler can transport about 50-100 distribution poles. Although the power grid in Southwest Louisiana will lack the redundancies that are normally in place until the transmission system is in full operation, MISO is working closely with Entergy and others to maintain system stability in the meantime.

How did MISO prepare for the emergency?

MISO began preparations about one week prior to anticipated landfall, including activation of our Hurricane Action Plan (HAP), which prescribes the following actions: monitoring weather and load conditions; enacting Conservative Operations; establishing communication channels with impacted members, neighboring Reliability Coordinators and state commissions; delaying planned outages; and activating MISO's Incident Management Team.

After the storm subsided, what steps did MISO take?

Initially, MISO enacted Conservative Operations and issued Capacity Advisories to affected areas of its footprint. Once damage assessments concluded, all efforts focused on restoring generation, transmission and load. MISO reconfigured select reserve zones in its footprint to better manage reliability. This action was taken to address the tight supplies of electricity and reserves due to limited import capability and generation availability.

Have there been any changes in the Market?

Initially, MISO needed to make manual adjustments to its processes and systems. To promote greater consistency and efficiency in the affected areas, MISO activated a local import constraint to more accurately reflect system limitations and the scarcity and value of both energy and reserves in the affected areas. These system improvements served to automate these adjustments.

As restoration evolves, has MISO been able to forecast load?

Developing a load forecast for impacted areas has been challenging. In addition to the typical challenges presented by weather and the COVID-19 pandemic, the aftermath of Hurricane Laura introduced additional complications associated with the timing of load pick up, particularly industrial load as industrial processes may return in stages. To maintain system reliability, MISO is working with impacted members to bring on additional load during off-peak hours when the system is more stable and system operators can monitor usage patterns prior to preparing the load forecast for peak conditions.

When will restoration be complete?

Substantial restoration efforts have been conducted in the first 30 days; however, due to the catastrophic damage in the Southeastern Texas and Southwestern Louisiana areas of the MISO footprint, comprehensive restoration of the most heavily damaged areas will require nearly a complete rebuild and could take weeks. On a positive note, restoration in Arkansas, Texas, and North Louisiana is complete for all customers who can take service.

The Lighthouse

By Lew Folkerth, Principal Reliability Consultant

Incident Response and Incident Management

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.

What's New in CIP-008-6?

CIP-008-6 will become effective on January 1, 2021. Changes in CIP-008-6 include:

- Electronic Access Control or Monitoring Systems (EACMS) are explicitly included in the Applicable Systems. This will include Intermediate Systems used for Interactive Remote Access and Electronic Security Perimeter boundary devices such as firewalls.
- The definitions "Cyber Security Incident" and "Reportable Cyber Security Incident" have changed to clarify that they apply to BES Cyber Systems at all impact levels. They also clarify that references to Electronic Security Perimeter, Physical Security Perimeter, and EACMS apply to high and medium impact BES Cyber Systems only.
- Your incident response plan now explicitly requires you to evaluate and define "attempts to compromise."
- Your incident response plan must include a process to determine if an event is an incident, a Cyber Security Incident, a Cyber Security Incident that was an attempt to compromise an Applicable System, or a Reportable Cyber Security Incident.
- You must use your incident response plan when responding to an attempt to compromise an Applicable System.
- You must retain records of your response to attempts to compromise an Applicable System.
- The new Requirement R4 contains explicit reporting language:
  - You must report Reportable Cyber Security Incidents and attempts to compromise an Applicable System.
  - Your incident reports must include certain specific information.
  - There are specified timelines for reporting:
    - Reportable Cyber Security Incident: 1 hour;
    - An attempt to compromise an Applicable System: Next calendar day;
    - Information updates: 7 calendar days.

As always, carefully read the enforceable language of the Standard (Requirements including referenced attachments, Applicability, Effective Date and Glossary terms) and base your compliance program on that language.

Big Sable Point, MI – Photo: L Folkerth

Also, there is a proposed Implementation Guidance document (not ERO approved as of this writing) that provides an overview of the structure and techniques for implementing CIP-008-6.

Low Impact

CIP-003-8, (Security Management Controls) Attachment 1 Section 4 uses the definitions for Cyber Security Incident and Reportable Cyber Security Incident. Even though CIP-003-8 doesn't

Continued on page 8

Continued from page 7

change on January 1, 2021, these definitions change and will be applicable to your CIP-003-8 compliance programs:

- The new definitions clarify that the Electronic Security Perimeter and Physical Security Perimeter language only applies to high and medium impact BES Cyber Systems.
- The term Reportable Cyber Security Incident now explicitly references BES Cyber Systems. You should know which systems owned by your entity are low impact BES Cyber Systems for incident reporting purposes. You can't just rely on asset-level determinations and still be consistent with the language of Section 4 and the Glossary.

CIP-005-6

The new language in CIP-005-6, contained in Parts 2.4 and 2.5, requires that you have the ability to "determine" and "disable" remote vendor connections. You may want to incorporate language to respond to Parts 2.4 and 2.5 in the appropriate incident response plan.

If an unauthorized party succeeds in exploiting a remote vendor connection, and that exploit results in the connection being disabled per CIP-005-6 Part 2.5, this will almost certainly meet the definition of a Reportable Cyber Security Incident and will require activation of your incident response plan. It would be prudent to have these actions already incorporated into your incident response plan.

Incident Management and Incident Response

The concept of incident response as applied to operational cyber assets has been around for decades. The concept of incident management began to be applied to these assets only in the last few years. Incident management is the art and science of providing leadership and pre-established processes to support incident response personnel. Incident management began in the 1970's with firefighters at California wildfires, but has been expanded and adopted in many areas. Electric utilities usually have mature incident management programs for disaster or storm response, but have not usually applied these techniques to Cyber Security Incidents.

If you want to learn more about incident management, I suggest the book "Incident Management for Operations" (Schnepp, Vidal & Hawley, O'Reilly 2017) as a good place to start. For example, one section explains the incident command structure and why such a structure is needed for incident response.

There is also an initiative underway to formally adapt incident management techniques to our operational control systems. Incident Command System for Industrial Control Systems (ICS4ICS) is being developed to bring the concepts of incident management to all aspects of our control systems. A good introduction to this concept, including links to FEMA advanced training on incident management, was presented by Megan Samford at the S4x20 industrial control system security conference. The video is available here.

CYPRES Report

FERC recently released a new study, "Cyber Planning for Response and Recovery Study (CYPRES)," available here. This document is a report based on observations from interviews of electric utilities by a joint team from FERC, NERC and Regional Entities. "Key Take-Aways" identified throughout the report may help you strengthen your incident response and recovery plans.

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.

An expanded version of this article, "CIP-012-1 In Depth," is available in the RF CIP Knowledge Center. Back issues of The Lighthouse, expanded articles and reference documents are also available.

Feedback

Please provide any feedback you may have on these articles. Suggestions for topics are always welcome and appreciated.

Lew Folkerth, Principal Reliability Consultant, I may be reached here.

Regulatory Affairs

FERC Staff Report on Lessons Learned from CIP Reliability Audits

FERC staff (FERC) recently released a report summarizing lessons learned from FERC-led nonpublic CIP audits of registered entities that took place in Fiscal Year 2020. During these audits, FERC found some potential noncompliances, but found that most registered entities met the requirements of the CIP Standards. FERC also observed voluntary practices that could improve the security of the Bulk Power System. The report discusses 12 lessons learned, which touch on issues found, voluntary best practices, and recommendations for assessments of risk and compliance. The 12 lessons learned are:

1. Ensure that all BES Cyber Assets are properly identified.
2. Ensure that all substation BES Cyber Systems are properly categorized as high, medium, or low impact.
3. Ensure that electronic access to BES Cyber System Information (BCSI) is properly authorized and revoked.
4. Consider having a dedicated visitor log at each Physical Security Perimeter (PSP) access point.
5. Consider locking BES Cyber Systems' server racks where possible.
6. Inspect all Physical Security Perimeters (PSPs) periodically to ensure that no unidentified physical access points exist.
7. Review security patch management processes periodically and ensure that they are implemented properly.
8. Consider consolidating and centralizing password change procedures and documentation.
9. Ensure that backup and recovery procedures are updated in a timely manner.
10. Ensure that all remediation plans and steps taken to mitigate vulnerabilities are documented.
11. Ensure that all procedures for tracking the reuse and disposal of substation assets are reviewed and updated regularly.
12. Consider evaluating the security controls implemented by third parties regularly and implement additional controls where needed when using a third party to manage BES Cyber System Information (BCSI).

FERC, NERC, and Regional Entities Report on Cyber Planning for Response and Recovery Study (CYPRES)

FERC, NERC and the Regions (the Joint Team) undertook a Cyber Planning for Response and Recovery Study (CYPRES) to assess the planning and readiness of electric utilities to respond to and recover from a cyber-security incident. The Joint Team conducted site visits to interview employees who oversee restoration and recovery planning at eight entities varying in size and function.

In September, the Joint Team issued a report discussing the results of this effort. The report contains key takeaways on creating and implementing incident response and recovery (IRR) plans, based on the phases of the incident response process:

Preparation, Detection and Analysis

- Effective IRR plans contain well-defined personnel roles, promote accountability, and, where appropriate, empower personnel to take action without unnecessary delays.
- Effective IRR plans leverage technology and automated tools while recognizing the importance of human performance.
- Effective implementation of IRR plans requires well-trained personnel who are constantly updating their skills.
- Effective IRR plans incorporate lessons learned from past cyber security incidents or tests.
- Baselining is an effective resource utilization tool that allows personnel to detect significant deviations from normal operations.
- Flow-charts or decision trees are useful to determine quickly when a predefined risk threshold is reached.

Containment and Eradication

- If an IRR plan containment strategy includes islanding operational networks, there should be a thorough understanding of the potential impact of such a decision.
- IRR plans should consider the possibility that a containment strategy may trigger predefined destructive actions by the malware.
- Evidence collection and continued analysis are important to determine whether an event is an indicator of a larger compromise.

Post-Incident Activity

- Effective IRR plans implement lessons learned from previous incidents and simulated activities identifying clear shortfalls in the IRR plan.

Regulatory Affairs

FERC Notice of Inquiry on Equipment and Services Produced or Provided by Certain Entities Identified as Risks to National Security

On September 17, 2020, FERC issued a Notice of Inquiry on Equipment and Services Produced or Provided by Certain Entities Identified as Risks to National Security (NOI).[1] In the NOI, FERC notes that it approved the first set of supply chain risk management standards in Order No. 850[2] in 2018, and that since that time, there have been significant developments in the form of Executive Orders, legislation and federal agency actions that raise concerns over the use of equipment and services provided by certain entities identified as risks to national security. Specifically, Huawei Technologies Company (Huawei) and ZTE Corporation (ZTE) have been identified as examples of such entities because they provide communication systems and other equipment and services that are critical to BES reliability. FERC states that there are many manufacturers of networking and telecommunications equipment, but Huawei, ZTE, and their subsidiaries are gaining substantial shares of the market globally. There are also Huawei and ZTE components embedded in equipment produced by unaffiliated vendors, which may be harder to identify within electric infrastructure but still present the same risks as hardware purchased directly from Huawei or ZTE.

Therefore, in the NOI, FERC is seeking comments on:

1. the extent of the use of equipment and services provided by certain entities (such as Huawei and ZTE) identified as risks to national security related to BES operations;
2. the risks to BES reliability and security posed by the use of equipment and services provided by certain entities;
3. whether the CIP Standards adequately mitigate the identified risks;
4. what mandatory actions FERC could consider taking to mitigate the risk of equipment and services provided by certain entities related to BES operations;
5. strategies that entities have implemented or plan to implement – in addition to compliance with the CIP Standards – to mitigate the risks associated with use of equipment and services provided by certain entities; and
6. other methods FERC may employ to address this matter including working collaboratively with industry to raise awareness about the identified risks and assisting with mitigating actions (i.e., such as facilitating information sharing).

[1] 172 FERC ¶ 61,224 (2020)

[2] Supply Chain Risk Management Reliability Standards, Order No. 850, 165 FERC ¶ 61,020 (2018)

3 172 FERC ¶ 61,225 (2020)

FERC Order No. 873 Approves Retirements of 18 Reliability Standard Requirements

In Order No. 873,[3] FERC approved the retirement of 18 Reliability Standard requirements requested for retirement by NERC. FERC concluded that the 18 requirements:

(1) provide little or no reliability benefit;

(2) are administrative in nature or relate expressly to commercial or business practices; or

(3) are redundant with other Reliability Standards.

The Order does not address the proposed retirement of 56 requirements constituting the "MOD A" Reliability Standards.

The four Reliability Standards being eliminated in their entirety are FAC-013-2 (Assessment of Transfer Capability for the Near-term Transmission Planning Horizon), INT-004-3.1 (Dynamic Transfers), INT-010-2.1 (Interchange Initiation and Modification for Reliability), and MOD-020-0 (Providing Interruptible Demands and Direct Control Load Management Data to System Operations and Reliability Coordinators).

The five Reliability Standards being modified are INT-006-5 (Evaluation of Interchange Transactions), INT-009-3 (Implementation of Interchange), PRC-004-6 (Protection System Misoperation Identification and Correction), IRO-002-7 (Reliability Coordination—Monitoring and Analysis), and TOP-001-5 (Transmission Operations). FERC also remanded proposed Reliability Standard FAC-008-4 for further consideration by NERC.

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 Posts Additional Resource on Modifications to CIP Standards

NERC posted both the streaming webinar and slide presentation regarding virtualization concepts and potential CIP Standards modifications related thereto.

Notable NERC Filings

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

- NERC submitted its annual report to FERC regarding Wide-Area Analysis of Technical Feasibility Exceptions
- NERC submitted a compliance filing to FERC in response to the Commission's Five-Year Performance Review Order.
- NERC submitted an informational compliance filing as a status update on two standards development projects.

Notable FERC Filings

- FERC issued an order denying a complaint from Michael Mabee related to Reliability Standard CIP-013-1.
- FERC issued a Notice of Inquiry seeking comments on the potential dangers related to Supply Chain risk.

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. Recent activity includes:

Project	Action	Start/End Date
SERC Regional Reliability Standards Development Procedure	Comment Period	10/7/2020 - 11/20/2020
New Standards Projects		
Project 2019-03-Cyber Security Supply Chain Risks	Final Ballot	10/7/2020 - 10/16/2020
Recent and Upcoming Standards Enforcement Dates		
October 1, 2020	CIP-005-6 – Cyber Security – Electronic Security Perimeter(s); CIP-010-3 – Cyber Security – Configuration Change Management and Vulnerability Assessments; CIP-013-1 – Cyber Security – Supply Chain Risk Management	
January 1, 2021	PRC-002-2 – Disturbance Monitoring and Reporting Requirements (50% compliance for Requirements 2-4, 6-11); PRC-025-2 – Generator Relay Loadability, phased-in implementation of Attachment 1: Relay Settings, Table 1 Options 5b, 14b, 15b, and 16b by six months (January 1, 2021); CIP-008-6 – Cyber Security – Incident Reporting and Response Planning; PRC-012-2 – Remedial Action Schemes	
April 1, 2021	PER-006-1 – Specific Training for Personnel; PRC-027-1 – Coordination of Protection Systems for Performance during Faults	
July 1, 2021	TPL-007-3 – Transmission System Planned Performance for Geomagnetic Disturbance Events (Requirements 11 and 12)	
January 1, 2022	TPL-007-3 - Transmission System Planned Performance for Geomagnetic Disturbance Events (Requirements 6, 6.1-6.4, 10, 10.1-10.4)	
July 1, 2022	PRC-002-2 – Disturbance Monitoring and Reporting Requirements (100% compliance for Requirements 2-4, 6-11)	
January 1, 2023	TPL-007-3 – 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, 8.3, 8.4, and 8.4.1)	
January 1, 2024	TPL-007-3 – Transmission System Planned Performance for Geomagnetic Disturbance Events (Requirements R7, 7.1, 7.2, 7.3, 7.3.1–7.3.2, 7.4, 7.4.1–7.4.3, 7.5, and 7.5.1.)	

These effective dates can be found here.

Technical Talk with RF

ReliabilityFirst offers a regularly scheduled monthly call to provide Entities and stakeholders with a forum for addressing topics and questions relevant to reliability, resiliency and security. These calls are held on the third Monday of each month from 2:00 to 3:30 p.m. EST.

In addition to compliance-related content, these calls cover other risk areas, such as cyber security, misoperations, situational awareness and much more. Please invite your Operations, Planning, Cyber, Design, IT, and/or Maintenance personnel, if you see an agenda topic they would be interested in!

November Event Information

Monday, November 16, 2020
2:00 p.m. – 3:30 p.m. EST
Click here to join
Meeting Number: 172 257 0322
Meeting Password: 0123456789
Join by phone: 1-650-479-3207, Access Code: 172 257 0322
Please join us on Slido.com using**#TechTalkRF**as the event code

Tentative Agenda Topics

Cold Weather Readiness – Standard Authorization Request (SAR) Update

Don Urban – Principal Analyst, Risk Analysis & Mitigation

- Mr. Urban will provide an update on the proposed standard development project initiated to review and address the recommendations provided from the FERC and NERC report "The South Central United States Cold Weather Bulk Electronic System Event of January 17, 2018" to enhance the reliability of the BES during cold weather events through preparation.
- This presentation is especially relevant for Generator Owners and Operators, Reliability Coordinators, and Balancing Authorities preparing for extreme cold weather conditions.

Exercise Master Planner Database

Bheshaj Krishnappa – Program Manager, Risk & Resiliency

David Sopata – Principal Reliability Consultant, Entity Engagement

- Testing incident response plans for cyber and physical security scenarios can be a key factor to improving resiliency in the face of dynamic emerging threats. This presentation will focus on RF's efforts to develop a BES Exercise Master Planner Database tool with a variety of current Cyber/Physical security test cases, scenarios and injects which stakeholders can utilize to evaluate, benchmark and mature their incident preparedness and resilience.
- This presentation is especially relevant for all cyber and physical security personnel who are in charge of evaluating entity's incident response and preparedness posture.

Vegetation Management Update – Lessons Learned and Audit Approaches

Beth Rettig – Technical Auditor, Operations and Planning Compliance Monitoring

Johnny Gest – Manager, Engineering and System Performance

- Ms. Rettig and Mr. Gest will recap the trends, root causes and lessons learned from vegetation related outages in the RF footprint. They will share our audit approach regarding right-of-way visits and share how participating in the RF Community of Practice can help drive continuous improvement.
- This presentation is especially relevant for all Transmission Owners and Generator Owners responsible for managing vegetation and minimizing encroachments on or adjacent to transmission rights of way.

September and October Presentations

In case you missed the recent calls or would like to reference the slides, most of the materials presented are posted on the RF website.

- Low Impact CIP Self-Certifications presentation (under Documents tab) from members of RF's CIP Compliance Monitoring team, Bob Yates and Lindsey Mannion
- Cold Weather Readiness presentation (under Documents tab) from Don Urban, Principal Analyst, Risk Analysis & Mitigation
- Assist Visit presentation (under Documents tab) from Ron Ross, Senior Reliability Consultant, Entity Engagement

SERC and RF Collaborate on Supply Chain Risk Management Training

SERC and RF are collaborating on a series of self-learning modules relating to the new supply chain standard, CIP-013-1.

These modules – available here – are self-paced and may be taken in any order. Personnel associated with an entity registered with either SERC or RF may request a Certificate of Completion at the end of each module.

Topics currently available include: "Supply Chain Risk Management Overview" and "Supply Chain Standards: Past, Present, Future" with additional topics planned for release in the near future.

Fall 2020 Virtual Workshop Recap

Like the majority of events this year, both of RF's major two-day workshops were impacted by the pandemic. After needing to cancel the Annual Spring Workshop in April, we were thrilled with the success of our Fall Virtual Workshop, with 575 total attendees from 150 different organizations.

We pared two full days of content down to two half-day sessions, with the morning focused on Facility Ratings and the afternoon on Supply Chain. In addition to addressing updates to the NERC CMEP Practice Guide, members of RF staff covered Facility Ratings topics ranging from validation and verification to the commissioning process to internal controls.

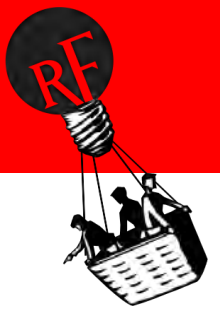
Many thanks to the presenters from AEP, PPL, CenterPoint Energy, Duquesne Light Company and Talen Energy for helping us close out the morning with Stakeholder Facility Ratings Successes and Lessons breakout sessions grouped by Small/Medium Transmission Owners, Large Transmission Owners and Generator Owners.

For the compliance-focused afternoon, attendees learned about entity Supply Chain programs and platforms, cross-Regional collaboration for Supply Chain training, as well as vendor metrics and risk assessment. In addition to an update from NERC and RF staff on the deferred Standard implementation and a preview of the forthcoming RF Supply Chain self-assessment tool, presentations from AEP, Fortress Information Security and Open Systems International rounded out a great day of timely information.

This workshop was a shining example of the collaboration we encourage throughout the RF footprint and industry as a whole, and we are proud of the overwhelmingly positive feedback we received. Attendees appreciated the half-day format with shorter presentations, the combination of pertinent topics, and the easily-applicable takeaways.

Receiving attendee feedback that "I'm wearing my fingers out taking notes" is a good-humored indicator that we're sharing highly relevant information. To that end, all of the presentations are posted under the Reliability Workshops tab on the Workshop Materials & Webinars page of our website.

Insider Threats Webinar Recap



Based on the fantastic attendee feedback and widespread interest, it's safe to say that RF's first-ever Insider Threats webinar last month won't be our last. Led by RF Resiliency & Risk Program Manager, Bheshaj Krishnappa, this half-day event brought together more than 200 attendees from 33 states and seven countries.

With an objective to improve awareness and share best practices, this informative session on Insider Threat risk management focused on trends, program management, lessons learned, resources and more.

The guest speaker presentations began with Dan Costa, Technical Manager at Carnegie Mellon Software Engineering Institute, discussing trends regarding the most prevalent Insider Threats in the energy sector, and Matt Shultz, IT Security Specialist at FERC, presenting a case study and resources for mitigating and reporting Insider Threats. Benjamin Gibson, Senior Physical Security Analyst at NERC/E-ISAC, provided guidance on what to do if you suspect an Insider Threat, and Steven McElwee, CISO at PJM, shared information on how to develop an Insider Threat Program.

Chad Connell, Senior Director of Cyber and Physical Security at MISO, followed with a discussion about detecting and defending against advanced cyber security threats, and the webinar finished with Mr. Krishnappa providing an overview of an eventual Insider Threat Program Maturity Framework tool to help users evaluate the status of their programs and benchmark performance over time.

In addition to the incredibly positive feedback, with participants saying the "four hours flew by" and it was "easily one of the best webinars I've attended in a long time," we received a great deal of interest in RF Insider Threat Program Maturity Assessment.

The presentation slides have been posted under the Webinars tab on the Workshop Materials & Webinars page of the RF website.

RF 3rd Annual HP Workshop Recap

RF held its 3rd Annual Human Performance (HP) Workshop at the end of August. This year's event was converted from its usual full-day, in-person format to a half-day webinar due to the pandemic, and more than 130 people attended.

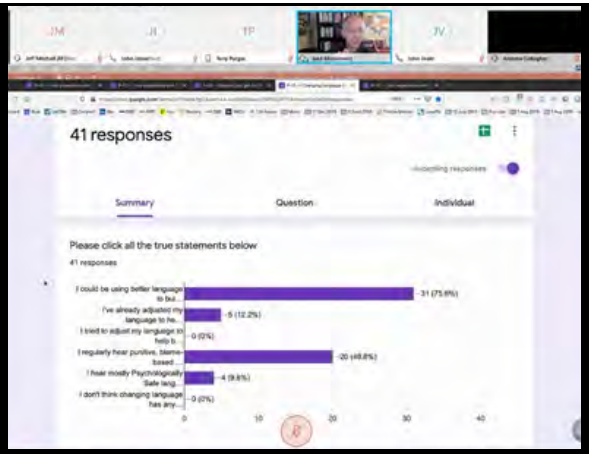
The workshop was headlined by HP professional Dr. Jake Mazulewicz, founder of JMA High Reliability Strategies, who shared strategies and techniques he has researched and developed to drive successful HP. Denise Hunter, Principal Technical Auditor at RF, discussed how internal controls dovetails with HP principals and concepts. Dave Sowers, co-founder of HP training provider Knowledge Vine, presented how risky behaviors plus a little bit of luck can still get good results. He explored the role of luck in keeping us safe, encouraging risky behaviors, and giving us a false sense of comfort. Mr. Sowers finished by taking a look at the big picture role of HP in eliminating the need for luck and how we can know if we are lucky or good.

A new addition to this year's program was a separate half-day session prior to the workshop for a Human Performance Improvement (HPI) Overview by Dr. Mazulewicz. This session was geared toward those who are new to the HP arena or who just want to refresh their knowledge of the principles and concepts.

These workshops are organized and coordinated by the Engineering and System Performance department to provide an opportunity for Registered Entity personnel to interact with their counterparts, learn new techniques and procedures, and share experiences.

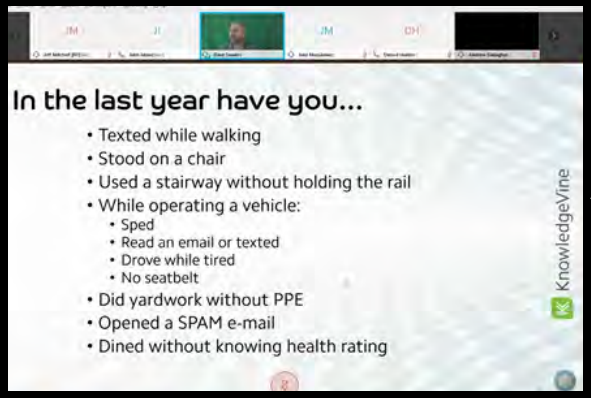
We were very pleased with all the positive comments from the attendee satisfaction survey, along with suggestions for future outreach efforts. A special thanks goes out to all those involved for their hard work in making these events a success.

This was truly a team effort!



Dr. Jake Mazulewicz shows the results of an interactive poll he conducted during the webinar.

Denise Hunter talks about some of the commonalities between internal controls and human performance principals.



Dave Sowers asks about some of the risky behaviors that you may have done in the past.

Calendar of Events

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

Date	RF Upcoming Events	Location
November 16	Technical Talk with RF	Conference Call
December 2	4th Quarter Board of Directors Committee Meetings	WebEx
December 3	Annual Meeting of Members and 4th Quarter Board of Directors Meeting	WebEx

Industry Events

Date	Industry Upcoming Events
October 15	NERC - 2020 Monitoring and Situational Awareness (M&SA) Technical Conference
October 27	FERC Technical Conference regarding Offshore Wind Integration in RTOs/ISOs (Docket Nol AD20-18-000) (Washington, DC)
October 29	PJM Members Committee Meeting
November 10	NERC - 2020 Monitoring and Situational Awareness (M&SA) Technical Conference
November 16	PJM MC Information Webinar
November 19	Virtual FERC Open Meeting
November 19	PJM Markets & Reliability Committee, Members Committee
December 10	MISO Annual Members Meeting and Board of Directors Meeting

ReliabilityFirst Members

AEP ENERGY PARTNERS
AES NORTH AMERICA GENERATION
ALLEGHENY ELECTRIC COOPERATIVE, INC
AMERICAN ELECTRIC POWER SERVICE CORP
AMERICAN TRANSMISSION CO, LLC
APPALACHIAN POWER COMPANY
BUCKEYE POWER INC
CALPINE ENERGY SERVICES, LP
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
EDISON MISSION MARKETING AND TRADING, INC.
EXELON CORPORATION
FIRSTENERGY SERVICES COMPANY
HAZELTON GENERATION LLC
HOOSIER ENERGY RURAL ELECTRIC COOPERATIVE, INC
ILLINOIS CITIZENS UTILITY BOARD
ILLINOIS MUNICIPAL ELECTRIC AGENCY
INDIANA MUNICIPAL POWER AGENCY
INDIANAPOLIS POWER & LIGHT COMPANY
INTERNATIONAL TRANSMISSION COMPANY

Forward Together RF ReliabilityFirst

LANSING BOARD OF WATER AND LIGHT
LINDEN VFT, LLC
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
VECTREN ENERGY DELIVERY OF INDIANA, INC
WABASH VALLEY POWER ASSOCIATION, INC
WISCONSIN ELECTRIC POWER COMPANY
WOLVERINE POWER SUPPLY COOPERATIVE, INC