Issue 5
2018 September/October

INSIDE THIS ISSUE

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

Follow us on:

Note from the President

Dear Stakeholders,

We have seen a lot of extreme weather lately, from hurricanes, floods, and record high temperatures, and many across the ERO are currently rising to the challenge of handling and recovering from extreme weather. As you will see from our cold weather preparedness update, I know efforts are already underway across the RF footprint to prepare for the winter ahead. The ongoing vigilance required to keep the lights on never ceases.

Accordingly, as we finally welcomed fall weather here in Ohio, the theme of this issue is to look at some of the looming threats that face our industry. While October is synonymous with ghosts and goblins, we are addressing some realistic frightening thoughts that may keep us up at night, such as: vegetation encroachment, patch and change management, compliance audits, and the changing generation mix. I'd like to draw your attention to our practical advice on how to reduce the risk of cyber-attacks by creating strong documentation around ports and services.

Day-to-day, I continue to be impressed with the work of our industry as we navigate all of these evolving risks. We discussed many of these at our Third Quarter Board meeting, with esteemed guests from NERC in attendance (*see recap on the next page*). At that meeting, the two RTOs in our Region graciously and thoroughly presented to our Board on the changing generation mix and how they are approaching and mitigating the risks in their territories. A few highlights from MISO are captured in this issue, The Seam.

I really appreciated seeing so many of you at our Fall Workshop last month, where many discussions around reliability and cyber risks and mitigation strategies occurred over the three days. The RF Protection System Subcommittee also recently met where they are actively working to lessen the risk of misoperations in our Region, through education and peer review.

I will echo the sentiment that Jim Robb shared with our Board, that in our industry, we are only as reliable as our weakest link. I appreciate all the efforts each of you are all taking to remain diligent and vigilant, and we at RF will keep working to help you stay on top of addressing those threats and risks the best we can.

Forward Together,

Tim

From the Board

Jim Robb

George Hawkins

Brian Fitzpatrick

Lori Spence

We were pleased to have Jim Robb, President & CEO of NERC, and George Hawkins, NERC Board of Trustees, in attendance at our Third Quarter Board Meeting to deliver opening keynotes.

Mr. Robb referenced the progress NERC has made to build a cohesive leadership team at NERC and acknowledged the progress the Regions have made as the ERO morphed into risk-based monitoring and enforcement while committing to build aligned and consistent practices.

He discussed his priorities, such as continuing to drive risks based thinking in all of our work and focusing on supporting the varying needs of the industry. Mr. Robb also highlighted the recent improvements at EISAC with the appointment of Bill Lawrence as the new security officer. He noted his user friendliness and as they recently completed their strategic plan, he believes it is apparent that Lawrence really understands that EISAC is an industry service function.

Mr. Robb discussed the expectation that RF will play an important role as it sits at the epicenter of a number of important issues, including baseload retirement, rise in natural gas generation, and working with multiple Reliability Coordinators. He also commended RF's leadership, work around data analytics, staffing decisions, risk assessment efforts and our history of collaboration with NERC and the other Regions.

Mr. Hawkins shared his background at DC Water to emphasize how the work we do with electricity is fundamental to everything else. He also expressed he has never seen a Board harder working or more prepared than the NERC board.

The Third Quarter meeting also included a training session on Resilience and Natural Gas Interdependencies provided by Brian Fitzpatrick, PJM Interconnection, and Lori Spence, Midcontinent Independent System Operator, Inc (MISO). They discussed their respective analyses concerning the grid's increased and growing interdependencies on natural gas.

Trump Hotel
1100 Pennsylvania Avenue N.W.
Washington, DC 20004

Click below for meeting details and registration:

Meeting Link

Ports and Services

By: Ron Ross, Senior Technical Auditor

As cyber attacks become more prevalent and sophisticated, it is increasingly clear that systems must be protected by robust defenses, knowledgeable and proactive personnel and sufficient documentation. Why is documentation included in those protections? Proper documentation is important in understanding how cyber assets are configured and their expected behavior. While sometimes compliance documentation may seem onerous, there is a reason – to protect the BES Cyber Systems that are used to protect and operate the Bulk Power System (BPS). The risk of a cyber asset security incident including compromise without knowledge of the compromise increases if system documentation is not accurate or adequate.

RF CIP Auditors examine a great amount of documentation and evidence of varying detail. One area requiring strong documentation, and discussed in the article is that of ports and services (CIP-007-6 R1 P1.1 & CIP-010-2 R1 P1.1). First, as a cybersecurity best practice, unnecessary ports and services should be disabled as part of system hardening routines to reduce the potential attack surface of the asset. It is important that required ports and services are thoroughly documented so that there is a clear understanding of 1) what ports should be enabled or open; 2) which services should be active, and 3) why those ports and services should be open and active. As a result, ports and services identified as open and active outside of what is documented can be identified and investigated for compromise or closed if not needed.

In the TCP/IP communications protocol world, logical ports are used to communicate between clients and servers across a network. These logical ports are defined by the services and applications that require this network communication. The ports used by these services and applications are typically defined by the Internet Assigned Numbers Authority (IANA). IANA has assigned standard service ports and suggested ranges where the operating system and application vendors can communicate without going through the process of requesting a formal port designation. Standard services will open specific listening ports based on their IANA assigned port. For example, the http services will typically use port 80/tcp for plaintext http or 443/tcp for encrypted https. This ensures that when making a request from a server that it will be available. Imagine trying to access https://www.google.com, for instance, but Google decided to put all of their web services on port 9123 (and didn't tell anyone or provide a redirection), you would never connect and you would not know why. In some cases, applications or services will use a range of ports to perform their network duties.

There are three types of logical ports:

- **Privileged ports** – These are ports that are within the range 0-1024. They are sometimes called system or well-known ports. At one time, Unix operating systems would only let the root account run processes within this range, hence the name privileged. Other operating systems followed suit and only permitted administrator level accounts to open ports within this range.
- **User or registered ports** – These are the ports that comprise the range 1025-49151. In this range, user created processes (not an administrator level created process) are freely able to open ports for network communication (whether listening or providing outbound communications to another system).
- In the case of privileged and registered ports, the IANA will typically approve and register the port for use by an application, if the developer or vendor request it.
- **Dynamic or private ports** – These are ports that comprise the range 49152-65535. Operating systems sometimes use these ports to allocate services that initially connect at a privileged or registered port and negotiate a connection in this range. These are sometimes referred to as ephemeral ports (*NB: some Linux kernels can use a range of 32768-61000, check your documentation*).

Documenting Logical Ports and Services

Let's begin simply and with some advice, if an application vendor lacks sufficient documentation and claims that their product can open any port: 1) it does not mean ports 1-65535; and 2) request that they verify with their development team. If 1-65535 is provided as the acceptable range for a service or application, sufficient and adequate documentation would be required at audit to justify this claim. Why is that? There are certain programing standards to ensure that applications interact well with other applications and the operating system itself. For example, if applications that provide different services are both vying for the same listening port, only the application that

Continued on page 4

Ports and Services

Continued from page 3

starts or accesses the port first will be listening and the other application could fail.

Applications or services that do not have an officially assigned port number should, as a best practice, use a port(s) somewhere in the range from 1025-65535. Vendors should be able to provide documentation of the services that open logical listening ports, which port(s) the service listens on and why the port is needed. If a range is used by the services, the vendor should have documentation of those ranges. This is good practice if the services need to be available through a firewall, for example, to ensure that the services are always able to be contacted by client computers.

If you are required to create your own documentation, there are tools that can assist, such as netstat and lsof. These tools or utilities can be executed on a host computer to quickly identify the logical ports and associated services. Also externally, nmap or other network-based port scanners can identify logical ports that are listening. One word of caution though, in many cases the network-based scanners will simply list the service associated that is on the IANA registered ports list. So, once the ports are determined, review of vendor documentation or contact with the vendor to provide documentation should be performed.

The following is an example of inadequate documentation of logical ports and services:

Service: ThisApplicationService
Port: 6915/tcp
Description: ThisApplicationService

Now, let's look at a few good examples of documenting logical ports and services:

1. **Service: MyApplicationService**
   Port: 5001/tcp
   Description: Provides MyApplication services to clients for telemetry data.

2. **Service: MyApplicationService2**
   Port: 5005/tcp-5050/tcp
   Description: Listens for updates from clients providing MyApplication weather condition data. A port in the range 5006-5050 is available to each client, once the initial connection is made to the port 5005/tcp.

Note that, in the above examples, the service listening on one port (5001/tcp) only requires a simple explanation in the description. The second service requires more explanation in the description due to the ability to listen on multiple ports (5005-5050/tcp).

Operating systems use port ranges as well for numerous services that are built-in. For example, recent versions of Microsoft Windows (both server and client operating systems) will use 49152-65535 for randomly allocated Remote Procedure Call (RPC) or Distributed Component Object Model (DCOM) services. In this case, the client computer could contact the server on port 135/tcp and be redirected to the randomly allocated port in the 49152-65535 range. If the service you are documenting is listening on a logical port within this range, it would be prudent to document that range for the service (with a good description and business justification, of course).

Going back to Microsoft Windows, when documenting svchost.exe, keep in mind that svchost.exe actually calls multiple dynamic-link libraries (dll) that open ports and provide various services. This will be listed when performing a 'netstat –anb' on the system. As an example of output from this command, one would see the following among the listing of ports:

Proto	Local Address	Foreign Address	State
[...]			
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING
EventLog			
[svchost.exe]			

In this case, EventLog is the service called by svchost.exe. Documentation should include the reason for the logical port/service and that the service is EventLog [svchost.exe], the EventLog service, not just svchost.exe as there is much more involved in the actual service.

Detailed below are a few resources for assistance in documenting logical ports and services:

- Example 1 - here
- Example 2 - here
- Isof man page - here

In addition, Google or other search engines can be your friend when documenting logical ports and services.

For further information or questions, you can always schedule an assist visit with our Entity Development team here.

Do You Know Where Your Vegetation Is?

By: Glen Kaht, Principal Technical Auditor

For personnel responsible for compliance with FAC-003-4 (Transmission Vegetation Management), one of the realities is that a vegetation-related outage could occur at any time. These personnel may have trouble sleeping at night if unanswered questions keep running through their mind:

- Are all of my transmission line Right-of-Ways (ROWs) within my transmission vegetation management program (TVMP)?
- Are my maintenance strategies/procedures/processes/specifications used to prevent the encroachment of vegetation into the Minimum Vegetation Clearance Distance (MVCD) sufficient?
- Are my Vegetation Inspections identifying all potential vegetation issues? Is my vegetation work plan effective to prevent vegetation issues until the next Vegetation Inspection?
- Is there a tree just inches away from causing a flash-over and a vegetation-related Sustained Outage?

These are scary thoughts indeed, but this article will offer some suggestions that might allay these nagging questions and help one to sleep soundly.

A vegetation-related Sustained Outage can result in serious consequences. In the worst case, it might cause or contribute to a Cascading event. Even without a Cascading event, a vegetation-related Sustained Outage will generate regulatory scrutiny, with the possibility of a significant monetary penalty.

The ERO has seen an increase in transmission outages caused by vegetation encroachment. This increase is a reminder that all affected Transmission Owners (TO) and Generator Owners (GO) need to be vigilant and implement controls to prevent transmission outages caused by vegetation. It should be noted that some of the Requirements themselves are controls, but additional controls will greatly aid in achieving the desired outcome.

Any of the following events are a violation of FAC-003-4:

- An encroachment into the MVCD,
- An encroachment due to a fall-in from inside the ROW that caused a vegetation-related Sustained Outage,
- An encroachment due to the blowing together of applicable lines and vegetation located inside the ROW that caused a vegetation-related Sustained Outage, or
- An encroachment due to vegetation growth into the MVCD that caused a vegetation-related Sustained Outage.

It should be emphasized that all of the above events are preventable. The only positive outcome from past violations is that we can learn from them, and take action to avoid similar events in the future. Some of what we have learned from our entities is discussed below.

First, it is critical to have a complete inventory of transmission line ROWs within the TVMP. If a transmission line ROW is not within the TVMP, then a Vegetation Inspection (R6) of that transmission line, or vegetation work (R7) on that transmission line are not going to occur, which significantly increases the likelihood that one of the events listed above will occur.

The possibility of an incomplete inventory of all transmission line ROWs within the TVMP increases as the number of transmission line ROWs increase. It is much easier to have an accurate inventory of 2 items than it is to have an accurate inventory of hundreds of items.

Next, maintenance strategies/procedures/processes/specifications used to prevent the encroachment of vegetation into the MVCD must be properly designed and documented (R3). Each TO and GO must develop and implement the strategies/procedures/processes/specifications as appropriate to their particular circumstances.

A TO with hundreds of miles of transmission line ROWs that have fast growing vegetation in remote areas with mountainous terrain will likely have different strategies/procedures/processes/specifications than a TO or GO with low lengths of transmission line ROWs that have slow growing vegetation in open fields has.

Continued on page 6

Do You Know Where Your Vegetation Is?

Continued from page 5

Vegetation Inspections (R6) offer the best opportunity to prevent the events listed earlier. More frequent Vegetation Inspections (where appropriate) can identify vegetation issues before they become an event. Past events have shown that some Vegetation Inspections did not identify vegetation issues that ultimately resulted in an event.

As one example, experience has shown that when performing visual inspections via helicopter patrols, in some instances vegetation clearances appear to be satisfactory when viewed from one direction, but are not satisfactory when viewed from a different direction.

The use and application of Light Detection and Ranging (LiDAR) has been extensively discussed within the ERO Enterprise and the industry. LiDAR can be very effective in identifying vegetation issues that a visual inspection may not identify. Many research papers have been written on practices and shortcomings in visual inspections of clearances between conductors and vegetation.

The scope of this article does not permit a review of these research papers and the practices and shortcomings, but RF encourages all entities (but especially those with extensive and/or complex transmission ROWs) to review some of the research papers and apply best practices to perform high quality Vegetation Inspections in order to achieve the desired results.

Examples of these research papers include (and are available on the NERC website):

- JOINT U.S.-CANADA POWER SYSTEM OUTAGE TASK FORCE UTILITY VEGETATION MANAGEMENT INITIAL REPORT - December 2003
- Transmission Vegetation Management Standard FAC-003-2 Technical Reference – September 30, 2011
- Maintaining Transmission Line Ratings Consistent with As-built Conditions Good Utility Practices - December 2015

Completion of the annual vegetation work plan of applicable lines (R7) will help ensure that no vegetation encroachments occur within the MVCD. Performance of the work plan must be in accordance with the maintenance strategies/procedures/processes/specifications that were previously discussed. After the vegetation clearance work has been completed, it is a best practice and a strong control to independently confirm that the vegetation work was performed as required and per the expectations of the TO/GO.

While the focus of this article is to identify and discuss issues associated with vegetation-related transmission events, it should be apparent that properly designed and implemented internal controls will achieve the desired outcome, and avoid undesired events.

Successful implementation of all aspects of a strong TVMP can be a complex (and expensive) endeavor, but the results are worth the effort. And it can alleviate nagging questions in the middle of the night, which should result in a nice, sound sleep.

Enforcement Update and Observations

By: Kristen Senk, Managing Counsel Enforcement

Overview of Enforcement Activity

Consistent with trends across the ERO, RF has experienced an increase in the number of violations identified since 2016.

As shown in Figure 1, the number of Operations and Planning violations has remained fairly consistent over the past several years. The driver for the increased volume is CIP, which was expected given the nature of CIP version 5, which went into effect in July, 2016.

However, despite the increased volume, detective controls seem to remain strong, as entities are self-identifying the majority of violations, and often times very quickly. Additionally, the majority of violations are lesser risk issues.

A Closer Look at CIP

Over half of the violations that RF has received in 2018 (through self-reports, audits, or otherwise) have been either **CIP-007** (specifically patch management) or **CIP-010** (change management).

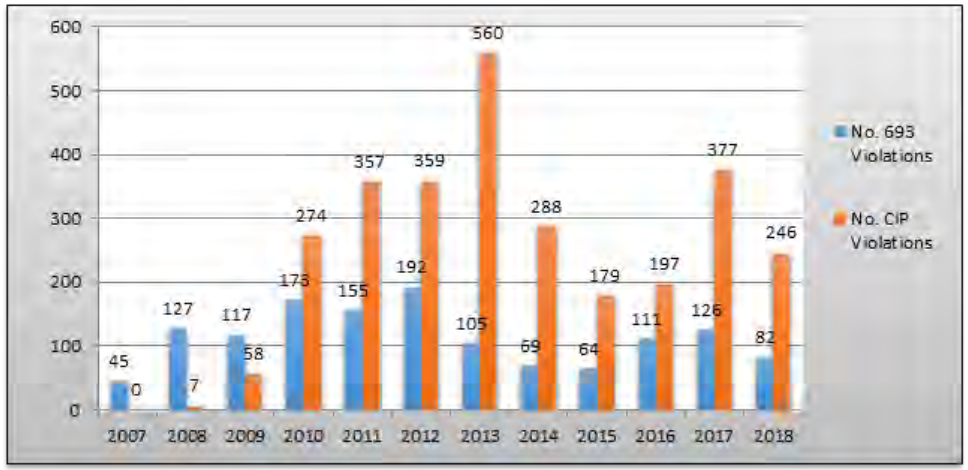


Figure 1

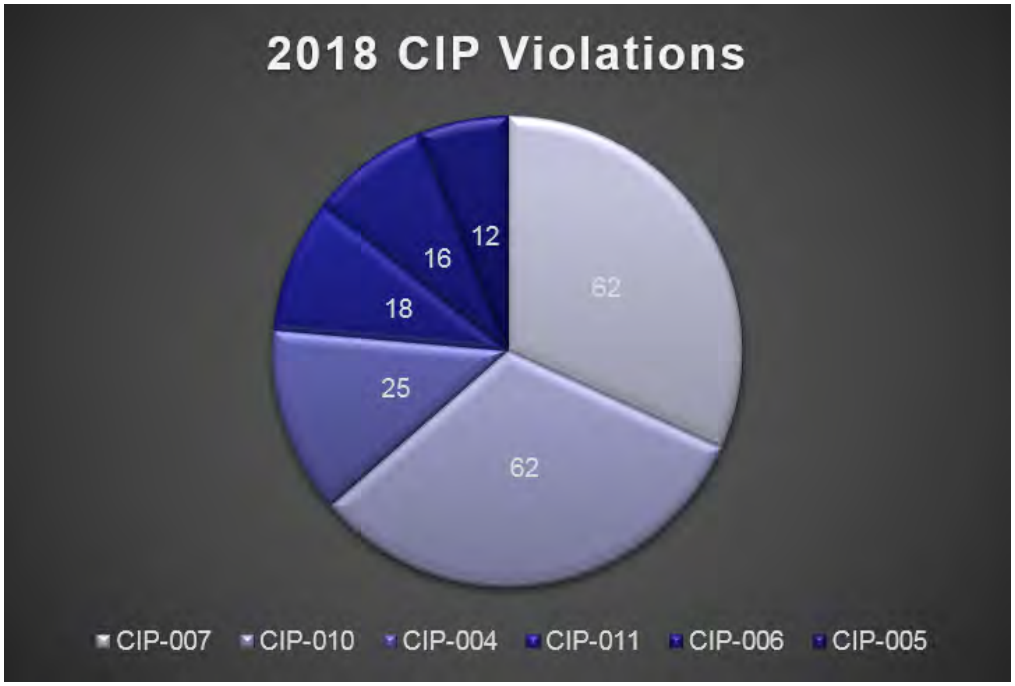


Figure 2

For this reason, and because of the criticality of the security measures covered by these Standards, CIP-007 and CIP-010 are focus areas for RF.

CIP-007 and CIP-010 govern high frequency conduct; that is, they cover multiple assets, people, and business units, and activity that occurs frequently. For this reason, we expect to see more noncompliances in these areas, especially for larger entities that manage thousands of assets and people, but sometimes for smaller entities as well.

In fact, sometimes, noncompliances in these focus areas can be an indication of a healthy compliance and security program, especially where entities are

Continued on page 8

Enforcement Update and Observations

Continued from page 7

quickly detecting and correcting the issues. However, it's important to note that where entities have experienced significant program deficiencies, CIP-007 and CIP-010 tend to be areas where the entities are struggling.

To effectively manage CIP-007 and CIP-010 programs, because of the nature of these programs, entities need to be strong in asset and configuration management. Entities should also focus on breaking down silos across their organizations.

RF has processed many violations in these areas where the causes related to lack of communication or miscommunication between the multiple groups responsible for managing the assets.

A Closer Look at Operations and Planning

While the Operations and Planning noncompliances account for a relatively small portion of the total noncompliances we process, we would like to share some observations regarding the activity we're seeing with **Vegetation Management**, **Facility Ratings**, and **Protection System Maintenance and Testing**.

Regarding **Vegetation Management**, the ERO has experienced several sustained outages related to vegetation contacts in the past few years. In light of this activity and the criticality of vegetation management, RF will increase targeted and general outreach in this area and work with its entities, Regional partners, and NERC to share best practices and lessons learned.

Regarding **Facility Ratings** and **Protection System Maintenance and Testing**, although the overall number of noncompliances has not increased significantly over the past few years, the Regions have identified some significant cases in these areas. Still, the majority of the noncompliances in these areas tend to be minimal risk.

Regarding maintenance and testing, some entities are identifying equipment that has never been tested. Depending on the criticality of the equipment and other factors, these issues may pose a higher risk to the system.

These noncompliances are generally due to insufficient asset and configuration management practices relating to old equipment or incorporating new equipment or changes into the entities' maintenance and testing programs.

Similarly, with Facility Ratings, some entities are identifying equipment that was not part of the ratings calculations (such as jumpers, risers, or secondary equipment) or identifying errors in their methodologies for calculating ratings.

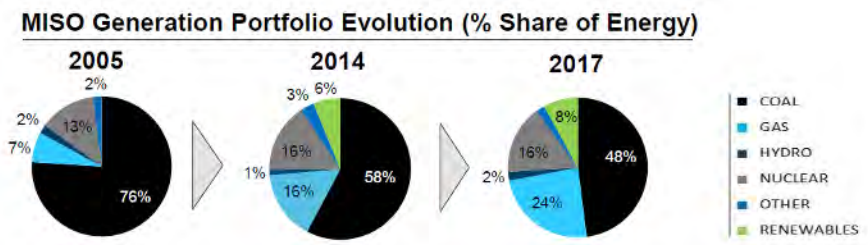
RF is working with the entities who have identified these noncompliances to understand the causes and ways to expedite identification of these issues in the future. Stay vigilant and stay tuned for more outreach activities in the coming months!

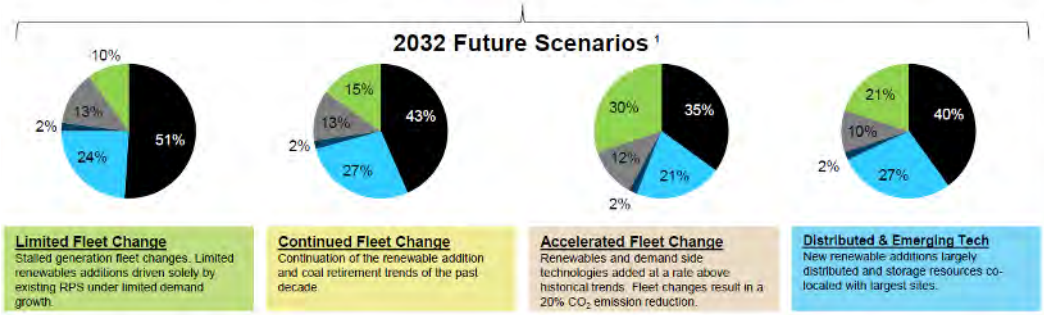
The Seam

By: MISO

Resilience and Natural Gas Dependencies

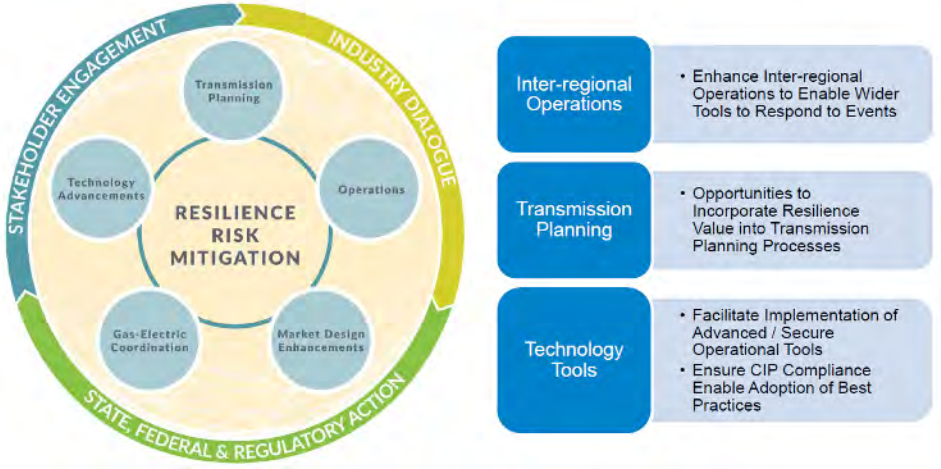
The Generation fleet in the MISO region has evolved substantially, primarily this evolution is from coal based generation to a lower carbon fleet. MISO efforts continue to anticipate and plan for the future, taking into account fleet changes and distributed and emerging technologies.





MISO works closely with its members and stakeholders to ensure grid reliability and resilience through developed tools and processes. An important part of addressing the changing generation and gas interdependencies is focusing on grid resilience. As you can see, the definition of resilience used is framed in such a way that it involves all NERC registered entities that have a role in grid reliability. It focuses on operations, ability to prepare, system planning, coordination, and recovery.

There are numerous opportunities for Future Industry Dialogue to Support Resilience. MISO has many activities underway to address gas electric challenges and support a resilient grid MISO continues to make steady progress on gas contingencies to assess potential reliability risk. Current planning studies have found no major reliability risk driven by gas pipeline contingencies evaluated. MISO's ongoing activities include study initiatives to assess additional gas disruptions.



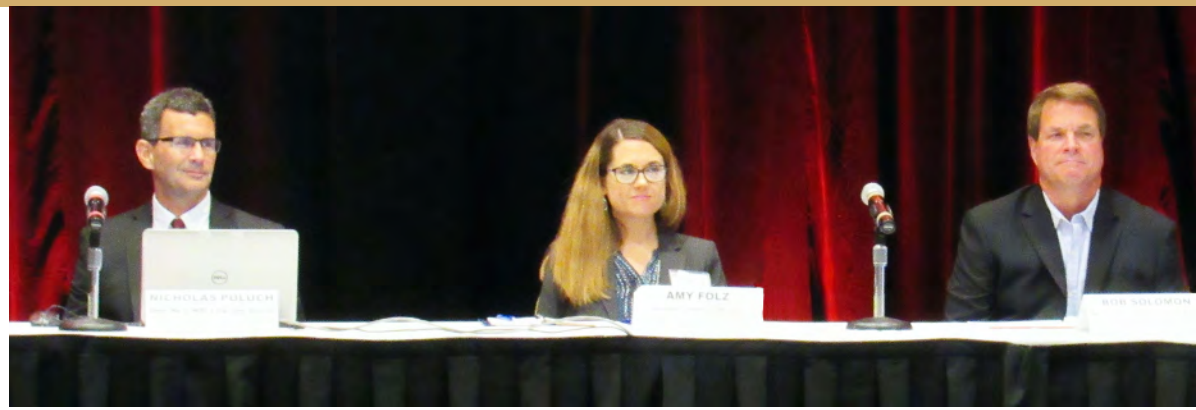
Internal Controls Review

By: Denise Hunter, Senior Technical Auditor

During the 2014 Fall Workshop, I presented on Internal Controls and the concept of Risk versus Compliance. The survey results of that presentation were less than stellar. The idea of internal controls and risk, and how they addressed reliability to the BES, seemed suspect. The region, as a whole, struggled to understand how those activities mitigated the risk identified by the Standard/Requirement and wondered "what about compliance?"

Fast forward four years to the 2018 Fall Workshop, and I had the honor to work with three companies that realize that mere compliance is a thing of the past and are working towards establishing internal control programs that include: identification of risks, mitigating their risks via internal controls, transparency of actions, and open dialogue to ensure understanding, coordination and cooperation throughout the region.

When I was asked to present at the Fall Workshop, I wrestled with coming up with a topic that I felt would move us to the next level. In previous workshops, I had detailed what an internal control was, what constituted a good one versus a weak one, and the objectives of internal controls.



From left tor right Nicholas Poluch, Amy Foltz, Bob Solomon

For this workshop I wanted to demonstrate what the review of an internal control would look like during an engagement such as an audit. The idea of a Mock Audit presented itself, but I wasn't sure I would find a single entity that would be willing to participate, so the idea shifted to a panel discussion.

A quick email was sent to a random selection of entities asking if anyone would be willing to "have a frank discussion regarding their internal controls" at the upcoming workshop. Before that day ended Nick Poluch at Talen Energy, Amy Folz with Vectren and Bob Soloman, Hoosier all stepped forward.

During our first meeting it became very apparent that Nick, Amy and Bob all agreed that sharing controls was necessary in order to proliferate a conversation detailing successes and failures of internal control design. Because of their enthusiasm regarding the topic, I decided to ask them if they would consider presenting our topic in a different manner: would they participate in a Mock Audit?

All three of them realized immediately what that meant: exposing their controls to scrutiny and comment by the entire region. It took about a minute before all of them said "Why not? Someone has to start the conversation."

The scope of the mock audit (PRC-005-6 R3, PRC-019-2 R1, VAR-002-4.1 R2) was based on standards and requirements that often present a challenge within our region.

I benefited greatly by participating in the Mock audit /Internal Controls discussion. The prep meetings with RF and the team allowed me to see the breath of internal controls that cover many different standards. It also provided me opportunity to practice articulating Talen's internal controls in a more concise fashion which worked out well for the RF presentation.

In addition, but just as important, I was able to present Talen's internal controls to Senior Management and NERC compliance team in a fashion that was easily understood and timely fashion.

One additional item, I learned that internal controls will change based on the risks at the time. Talen is a young company which is made up of several different companies. So the risks in the past couple years may not be the same risks that we see in the future. This was something you highlighted.

We are now looking to the future and are prepared to make changes the internal controls program based on future potential risks.

Nicholas Poluch, Senior Mgr. of NERC Eng. and Cyber Secuity, Talen Energy

TALEN ENERGY

Continued on page 11

Internal Controls Review

Continued from page 10

During the demonstration the following controls were discussed:

- Checklists: to assure all expected activities were performed.
- Contract management: necessary to manage the negotiation, execution, performance, modification and completion of contracts due to risk mitigation being provided by a third party.
- Data analysis: detailed review of data to determine mitigation of risk, trends and identify opportunities of improvement.
- Reviews: to ensure accuracy and completeness.
- Risk assessment: analysis of the adequacy of a process, set priorities for the organization, and determine the level of risk.
- Standardized documentation: mitigates the risk of information that is often presented in varying forms.

At the end of our hour it was apparent that the conversation had been started and a paradigm shift was occurring.

Now that the RF community of registered entities has seen the shift, it is ALL of our responsibility and duty to continue these open dialogues.

These conversations will help to promote our continuous improvement model around risk and internal controls and safeguard the reliability, security and resiliency of the Bulk Power System.

"This was a great opportunity for me to engage with RF staff and other utility experts, both on the panel and at the conference.

I value RF conferences as opportunities to share experiences, to connect with others in the regulated community and to positively impact electric reliability AND compliance."

Thanks for the opportunity.

Amy Foltz, Electric Reliability Compliance Mgr., Vectren Corporation

VECTREN
Live Smart

The Internal control portion of the RF Workshop was an excellent opportunity to discuss real examples of internal controls with Denise Hunter in a mock audit setting. This was an excellent next step in RF's efforts in assisting all of the entities at the workshop in the development of internal controls. Hoosier is eager to share and see examples of internal control from other entities in the RF footprint.

Any of the entities at the workshop are welcome to contact Hoosier Energy if they would like any of the material that was presented at the workshop. Hoosier Energy also benefited by participating in this exercise in regard to improving Hoosier's internal control program and analyzing risk.

Bob Solomon, Mgr., Compliance, NERC and Power Markets, Hoosier Energy

HOOSIERENERGY

The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

"Achieve the Objective…"

In this recurring column, I explore various CIP issues. I share with you my views and opinions, which are not binding, but rather are intended to provoke discussion within your entity and to be helpful to you as you and your entity 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 may also 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.

Q: How do I show an audit team that I have "achieved the objective" of a CIP Requirement?

A: Objective-based Standards

The ERO Enterprise (NERC and the Regions) has been trending toward objective-based Reliability Standards for many years. This trend appears to be gaining momentum, especially with the CIP Standards.

Some Requirements, such as CIP-010-3 R4, Transient Cyber Assets and Removable Media, explicitly use the phrase "achieve the objective" within the language of the Requirement. FERC stated recently, "We expect responsible entities to be able to provide a technically sound explanation as to how their electronic access controls meet the security objective." [Order 843 at P28, referring to electronic access controls for low impact BES Cyber Systems]

I recommend that you treat all of the CIP Standards as objective-based, and that you write your policies, plans, processes, and procedures from this perspective.

The shift toward objective-based Standards is good for security and also makes good business sense. Why spend money on compliance and security programs that do not result in a robust security posture? Why not maximize the benefit of compliance expenses by implementing good security practices that achieve the intended objective, and use compliance as the governing layer to ensure those security practices are followed rigorously? Compliance should be a by-product of a robust security program, not an end in itself.

As an example, an entity implemented a network backup system for its primary Control Center. The backup system uses a network-attached storage system, which stores the backed-up files for the entire Control Center. This arrangement meets the language of CIP-009-6, Recovery Plans for BES Cyber Systems, by providing for the backup and storage of information required for

Sand Hills Lighthouse, Ahmeek, MI – Photo: L Folkerth

recovery. However, online storage is subject to the threat posed by ransomware, which encrypts a victim's data and demands a ransom to provide decryption. If the Control Center's systems fall victim to this threat, the online backups that might be used to recover those systems could be encrypted as well. This would leave no way to recover the Control Center's systems without rebuilding those systems from scratch, a lengthy process which may result in a very different operating environment for the entity. If the entity had reviewed this approach against the objective of CIP-009-6, which might be stated as: "Be able to recover Control Center operability from any foreseeable event within a reasonable time," the entity would probably have seen the need for offline backups on its own.

Security Plan

In order to be able to demonstrate meeting objectives, your organization needs to have a documented plan in place. That plan needs to address all objective-based Requirements, but I recommend that you write your plan to address the objectives of all the Requirements that are applicable to you.

If you're subject to the CIP Standards, you already have a security plan that consists of a set of security processes tied together by a security policy. Let's build on this foundation to create a comprehensive security plan for your CIP assets.

Overall Security Objective

Your organization's security plan should include an objective for the plan as a whole. This overall objective will be the target all Requirement-based objectives

Continued on page 13

Continued from page 12

should support. For example, the overall objective for a Generator Operator might say, "Maintain the safety, operability, and integrity of ABC Generating Plant by rigorously implementing security practices that address the risk of compromise by a malicious actor or by inadvertent action."

I'll take this objective apart and explain what it means to me. I suggest that you perform this exercise for each of your objectives and keep the analysis in your documentation.

- "Maintain" implies a continuing process. Security is not something that you perform once and you're done. Security is an ongoing set of actions that adapt to changing conditions.
- "Safety" is always the first priority. I included safety here because safety instrumented systems have been successfully compromised by malicious actors.
- "Operability" of an asset is the ability to have control over the operation of that asset. If you lose operability, the consequences could be extreme. For example, a set of relays at multiple substations could be operated in a way to cause extended overload of a transformer or transmission line, perhaps resulting in destruction of that equipment.
- "Integrity" is the health of the asset as a whole. If integrity is compromised, the asset could be damaged, you may lose the benefit of the asset for an extended time, and you may incur substantial costs to repair the asset.
- "Rigorously implementing" means that security that is partially implemented, or implemented on an irregular schedule, may not be effective in preventing the asset from being compromised. For example, the Equifax breach was reportedly possible because one security patch was not applied to a server in a timely manner.
- "Security practices" are the actions specified in this security plan.
- "Address the risk" means to look at or pay attention to risk. It is impossible to eliminate all risk, so we prioritize where we spend our resources based on our evaluation of the risk involved.
- "Compromise" can be any condition that affects the function of the asset. This could involve denial of service, installation of malicious code, damage or destruction of physical equipment, and so on.
- "Malicious actor" can be an employee, contractor, vendor, activist, criminal, nation-state, and many others. Your security plan should evaluate the risk of each type of actor and implement protections based on the assessed risks.
- "Inadvertent action" means any action taken that has unintended adverse consequences. For example, NERC Lesson Learned LL20181001 (available here) discusses the loss of a SCADA system for several hours after a seemingly simple patch cable change.

This is a simplified example. You should adopt the overall security objective that works best for your organization.

Requirement-based Security Objectives

In order to achieve the overall security objective, specialized security objectives should be created to address particular areas of security. You can combine multiple CIP Requirements into a program group, such as ports and services, with a common objective. Or you can address the CIP Requirements individually.

For the discussion below, I'll assume we're looking at the Requirements individually. Make sure your security plan can answer the following questions for each Requirement:

1. **What is the security objective of this Requirement?**
   Try to state the security objective, as you believe it applies to you, clearly and succinctly. For example, I might state the security objective of CIP-002-5.1 R1, BES Cyber System Categorization, as, "Identify and categorize each device that could be susceptible to cyber compromise and that could have a reliability impact before manual intervention can override the compromised device."
2. **How will the security objective be met?**
   Your security plan must clearly show the steps you take to meet the security objective. You get to determine how you will achieve the objective, subject to review and assessment from an audit team. These steps will be what your performance is measured against, rather than a prescriptive requirement. For example, if your security plan calls for you to use application whitelisting to prevent malicious code, your audit will assess your effectiveness in the implementation of this approach.
3. **How will the security plan adapt to changing threats?**
   The threat environment changes far more quickly than Standards can be modified. Unless the standards development process changes, the CIP Standards will always lag far behind emerging threats. Therefore, it is important that your security plan is designed to recognize and deal

Continued on page 14

Continued from page 13

Internal Controls

If you want to learn more about internal controls, there are many sources of information. *Standards for Internal Control in the Federal Government* (the GAO "Green Book") is available here.

NERC's *ERO Enterprise Guide for Internal Controls* is available here.

If you are interested in a discussion of internal controls with RF staff, please request an Assist Visit. Details are at the end of this article.

with evolving threats. For example, your security plan might establish a threat analysis team that meets periodically to analyze changes to the threat environment and to plan responses to emerging or changing threats. In the CIP-009-6 R1 example I presented earlier, the entity designed the online backup scheme before the threat of ransomware became significant. A threat analysis team could have identified that threat as it became known and responded by ensuring an offline backup system was implemented to supplement the online backups.

4. **How will you measure performance of the plan?**
   Your security plan should include measures to provide reasonable assurance that the objectives of the plan will be achieved. This is one of the functions of internal controls. Your internal controls should be designed to identify potential problems before they become actual security or compliance issues. [See sidebar]

5. **How will you correct any shortcomings in the plan?**
   Especially in cyber security, plans can age and need updating. You should review your security plan and your performance measures periodically to ensure the plan is not beginning to weaken in any area. You will need to determine what the frequency of this review should be. This will depend on many factors, such as the emergence of new threats, changes in existing threats, the position of your entity within the BES, etc.

6. **Does the plan meet compliance requirements?**
   Whenever the plan changes, make sure you are still meeting the letter of each Requirement, in addition to your security objective. For example, an entity implemented application whitelisting to achieve the objective of preventing the introduction of unauthorized code into its systems. Since the entity achieved its objective in this way, the entity wanted to know if it could perform patch management on a quarterly cycle, rather than monthly. The audit teams have great flexibility, but the language of CIP-007-6 R2 is clear. The entity was advised to retain the monthly patch cycle until audit practices become sufficiently flexible to be able to permit alternate ways of achieving compliance.

7. **Will the plan produce sufficient, appropriate evidence of compliance?**
   For the prescriptive CIP Requirements, such as CIP-007-6 R2, Patch Management, make sure your security plan produces good quality evidence of compliance. As a guide to what evidence will be requested during an audit, Version 2 of the Evidence Request Tool is now available on the NERC web site. For objective-based CIP Requirements, such as CIP-007-6 R3, Malicious Code Prevention, produce documentation of the above six steps, with emphasis on steps 2 and 4. You can look at step 2 as providing the (self-imposed) prescriptive requirements that the objective-based Requirement lacks. Step 4 provides evidence that you are rigorously following the requirements you specified in step 2. Refer to the Evidence Request Tool for examples of the type of evidence needed to satisfy a prescriptive Requirement, and adapt these examples for your own use.

If you would like help in setting up a risk-based compliance program that addresses objective-based Standards and Requirements, or if you just want a different set of eyes to look at your work, you may request an Assist Visit via the web link below.

Requests for Assistance

If you are an entity registered within RF and believe you need assistance in sorting your way through this or any reliability-related issue, remember RF has the Assist Visit program. Submit an Assist Visit Request via the rfirst.org web site here.

Feedback

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

I may be reached here.

In the Industry

Letter Order Approving Amendments to NERC

On June 4, 2018, North American Electric Reliability Corporation ("NERC") submitted a petition requesting approval of amendments to NERC'S Bylaws. NERC proposed to amend Article V, Section 1 of the Bylaws to reduce the 5 day prior notice requirement for Board of Trustee ("Board") meetings. The amendment will allow for a 24 hour prior notice for special board meeting that are held in closed session.

The amendment does not affect the need to provide notice to the public and to members of any meetings, whether closed or open, 24 hours after notice is given to Board of Trustees.

NERC stated in its proposal that the shortened notice period will permit the Board to address matters that may be considered during a closed session in a timelier manner, while not changing the notice provided to stakeholders of any Board meeting.

On September 25, 2018 the Federal Energy Regulatory Commission ("FERC") issued a letter accepting the revisions to the NERC Bylaws. NERC's filing was accepted uncontested, and FERC's order constitutes a final agency action. Requests for rehearing by the Commission may be filed within 30 days of issuance of the order.

U.S. Senate Examines Blackstart Resource Capability

On October 11, 2018, the U.S Senate Committee on Energy and Natural Resources invited experts to testify about blackstart generation capacity. In the case of a system-wide blackout, utilities rely on blackstart resources to get larger generators back online to restore power. Blackstart units are typically small diesel or gas-fired generation units

The purpose of the hearing was to hear from utilities about the preparedness of the U.S. grid to restore service quickly after a widespread blackout.

Panelists at the hearing spoke positively about the resilience of the U.S. grid and its ability to recover from a widespread blackout. PJM President and CEO Andrew Ott and North American Transmission Forum President and CEO Thomas J. Galloway Sr. were among the panelists.

An archived webcast of the hearing is available here.

Regulatory Affairs

Trump Administration Releases National Cybersecurity Strategy

On September 21, 2018, the Trump Administration released its National Cybersecurity Strategy (Strategy). The Strategy is a statement of Administration policy and builds on prior efforts by the Obama Administration to develop a comprehensive and coherent nationwide cybersecurity strategy. The Strategy applies to the entire federal government and identifies four major areas of focus: Supply Chain Risk Management, Strengthening Information Sharing Efforts, Building a Robust Cybersecurity Workforce, and Deterrence and Offensive Capabilities. Some highlights of the Strategy include mandating federal investment in more secure supply chain technologies, sharing threat and vulnerability information with cleared information and communications technology providers, and authorizing federal agencies to conduct counter-offensive operations against malicious actors. The Strategy is available here.

Recent Weather Events Show Grid Resilience, Need for Flexibility: Glick

On September 20, 2018, FERC Commissioners discussed the power grid and its performance during recent weather events. Commissioner Richard Glick argued that Hurricane Florence showed the power system's resilience during extreme weather because the bulk system was largely unaffected, and that this highlights that resilience issues are primarily distribution issues and not bulk power issues.

As of September 19, 2018 the power demand in the hardest-hit area had bounced back to pre-storm levels, and the number of electricity consumers without power dropped below 180,000. The developers of gas pipelines in the region also reported that Florence had little to no effect on their projects.

Commissioner Glick also spoke about the hot temperatures that tested ISO New England on Labor Day (September 3). The peak load was more than 2,000 MW higher than the forecast causing energy prices to rise. This triggered ISO-NE's first pay-for-performance event. It penalized inflexible resources and rewarded those that could quickly respond. Glick stated that this incident highlights the need for flexibility. Glick has urged FERC to pursue improvements to market rules like pay-for-performance program rather than out-of-market solutions.

FERC Releases its Strategic Plan for Fiscal Years 2018-2022

At the end of September 2018, FERC released its Strategic Plan for Fiscal Years (FY) 2018-2022. This Strategic Plan builds on the success of FERC's previous Strategic Plan as the GPRA Modernization Act of 2010 requires FERC to update its Strategic Plan every four years. The Plan is designed to giver FERC's external stakeholders an understanding of FERC's authorities, priorities, and processes.

FERC's stated mission in the Plan is ensuring economically efficient, safe, reliable, and secure energy is provided for consumers at a reasonable cost. FERC's top three organizational goals, which are unchanged from the previous draft of the Strategic Plan that was released in 2014, are ensuring "just and reasonable" energy rates; promoting "safe, reliable, and secure infrastructure"; and preserving "organizational excellence" via its workforce and ethical standards.

In the Plan, FERC indicated it would increase cybersecurity inspections of dams, natural gas pipelines, and liquefied natural gas plants as these facilities are at an increased risk from new and evolving threats. The 2018 Strategic Plan is available here.

Standards Update

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

General NERC Standards News

New RSAWs posted

The following four new RSAWs are now posted on NERC's RSAWs page:

- BAL-005-1 (Balancing Authority Control) applies to Balancing Authorities and the effective date of the Standards is 1/1/2019. BAL-005-1 will replace BAL-005-0.2b and BAL-006-2.
- FAC-001-3 (Facility Interconnection Requirements) applies to Transmission Owners and applicable Generator Owners, and the effective date of the Standard is 1/1/2019. FAC-001-3 replaces FAC-001-2.
- The RSAWs for BAL-002-2(i) (Disturbance Control Performance – Contingency Reserve for Recovery from a Balancing Contingency Event) and PRC-025-2 (Generator Relay Loadability) are updated to reflect the correct names of the Standards.

Other Resources posted

NERC has posted the following resources:

- the streaming webinar and slide presentation for the Project 2015-10 Single Points of Failure webinar;
- the streaming webinar for the PER-006-1 Requirement Training webinar;
- the streaming webinar and slide presentation for the Functional Model Advisory Group Functional Model and Functional Model Technical Document Revisions webinar.

Notable NERC Filings

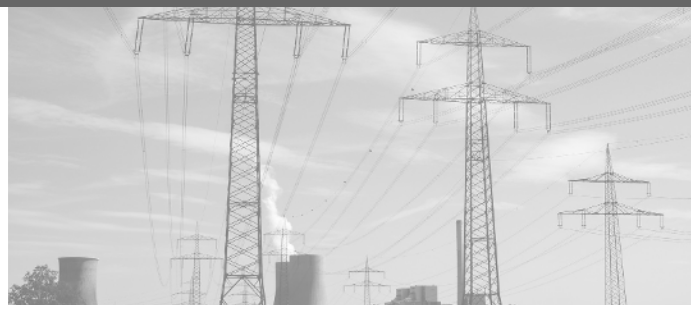
In August, NERC filed the following:

- a petition for the approval of proposed Reliability Standard BAL-002-3 (Disturbance Control Performance - Contingency reserve for Recovery from a Balancing Contingency Event), the Implementation Plan and the retirement of currently-effective Reliability Standard BAL-002-2.

In September, NERC filed the following:

- a petition for approval of proposed Reliability Standard VAR-001-5 (Voltage and Reactive Control); and,
- an informational filing regarding Proposed Supply Chain Risk Management Standards as directed by FERC in its NOPR on Jan. 18, 2018.

NERC's filings can be found here.



Notable FERC Issuances

In September, FERC issued the following:

- a letter order approving the Joint Petition submitted by NERC and WECC requesting the retirement of regional Reliability Standard VAR-002-WECC-2 (Automatic Voltage Regulators) effective immediately.

General FERC Standards News

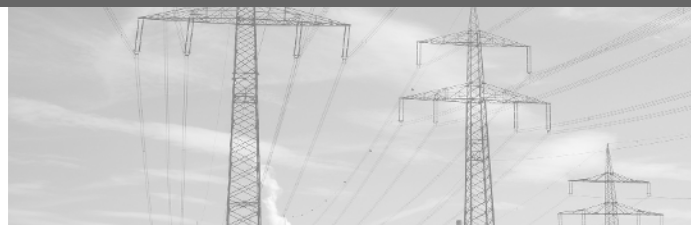
FERC, NERC Announce Joint Inquiry into Cold Weather Event

FERC and NERC have initiated a joint inquiry to assess the extreme cold weather event that occurred in the Midwest and a portion of South Central U.S. during the week of January 15, 2018. The inquiry will focus on identifying the causes of, and any contributing factors to, the event, and will identify any appropriate recommendations for improving operations under similar conditions.

This inquiry is not an enforcement investigation. FERC and NERC staff will work with the Midwest Reliability Organization, ReliabilityFirst, SERC Reliability Corporation, and the relevant involved companies.

Standards Update

New Standards Projects



Several new Standards projects and new project phases are underway. Projects are described on the NERC Standards website, along with links to all drafts, voting results, and similar materials. Recent additions include the following projects:

Project	Action	Start/End Date
2016-02 Modifications to CIP Standards (CIP-002-6 and CIP-003-8)	Initial Ballot & Non-Binding Polls	9/25/18 - 10/9/18
2015-09 Establish and Communicate System Operating Limits	Initial Ballot, Additional Ballots, and Non-Binding Polls	10/8/18 - 10/17/18

Other Active Comment Periods

Project	Action	Start/End Date
2016-02 Modifications to CIP Standards (CIP-002-6 and CIP-003-8)	Comment Period	8/23/18 - 10/9/18
2015-09 Establish and Communicate System Operating Limits	Comment Period	8/24/18 - 10/17/18

Recent and Upcoming Standards Enforcement Dates

January 1, 2019	BAL-005-1 – Balancing Authority Control; FAC-001-3 – Facility Interconnection Requirements; TPL-007-1 – Transmission System Planned Performance for Geomagnetic Disturbance Events (Requirements 5, 5.1-5.2)
April 1, 2019	EOP-004-4 – Event Reporting; EOP-005-3 – System Restoration from Blackstart Resources; EOP-006-3 – System Restoration Coordination; EOP-008-2 – Loss of Control Center Functionality
January 1, 2020	CIP-003-7 – Cyber Security – Security Management Controls; PRC-026-1 – Relay Performance During Stable Power Swings (Requirements 2-4)
July 1, 2020	PRC-002-2 – Disturbance Monitoring and Reporting Requirements (50% compliance for Requirements 2-4, 6-11)
October 1, 2020	PER-006-1 – Specific Training for Personnel ; PRC-027-1 – Coordination of Protection Systems for Performance during Faults
January 1, 2021	PRC-012-2 – Remedial Action Schemes

These effective dates can be found here.

2018 Fall Workshop

Thanks to everyone who participated in our 2018 Fall Workshop.

Our President and CEO, Tim Gallagher, opened the workshop with his thoughts on the current state of the region. Mr. Gallagher then introduced Jim Robb, President and Chief Executive Officer of the North American Electric Reliability Corporation (NERC).

Mr. Robb provided the audience with insight into the current status, challenges, and opportunities of the ERO. The rest of the morning consisted of presentations covering: internal controls during audit engagements, future operations, and planning standards that will be subject to enforcement.

After lunch, several presenters from NERC provided updates on current initiatives. Carter Edge discussed how certain features of the Organizational Certification Program are being proposed for amendment in the NERC Rules of Procedure and how entities can engage in commenting on the amendments.

NERC's Lonnie Ratliff followed and provided lessons learned during the recent Supply Chain Small Group Advisory sessions (SGAS). Lonnie also discussed the origins of CIP-013 and modifications to existing CIP Standards.

Day one of the workshop concluded with RF's Manager of Entity Development, Erik Johnson, providing an overview of RF's organization structure and introducing the various RF departments and their roles and responsibilities. He further described which activities are handled by each department to aid in navigating the organization.

Throughout the workshop, RF manned tables that enabled attendees to ask specific questions and obtain guidance and information from the departmental representatives.

At the end of day one, RF hosted a Social Hour for networking with both RF staff and attendees.

Day two of the workshop consisted of separate events for the Compliance User Group (CUG) and the Critical Infrastructure Protection Committee (CIPC) to provide information to and gain feedback from their members.

Day three of the Fall Workshop focused on key Critical Infrastructure Protection (CIP) programs and initiatives.

During the first session, RF's Ron Ross highlighted commonalities in RF regarding violations and audit findings within the CIP Standards. He focused on those standards and requirements that are most commonly violated or where deficiencies have been noted. He also gave examples of internal controls that, when implemented, can assist with compliance with the CIP Standards and Requirements.

Bob Yates (RF), followed and discussed the elements, functions, and uses of the new Attachment C for the ERO Request for Information workbook.

The morning continued with a panel of representatives from several regional entities sharing how they use a variety of tools to enhance compliance and security. This panel led by RF's Max Reisinger, included:

2018 Fall Workshop

Vectren's Jamie Young, AES' Chip Wenz, and FirstEnergy's Hugh R. Conley, Jr.

Closing out the morning session, RF's Shon Austin discussed the joint Technical Alert released by the DHS and FBI that described worldwide cyber-attacks from Russian state-sponsored cyber actors. The alert announced that the Russian sponsored cyber-attacks enabled intellectual property theft and espionage.

His presentation provided an understanding of vulnerabilities and tactics used by bad actors to access protected information and gave guidance on how to protect sensitive information by securing networks and devices. The afternoon consisted of several sessions from leading cyber security organizations.

The organization MITRE introduced the fundamental motivations and strategies behind nation-state adversaries and explained how supply chain, cyber-OT, cyber-IT, and the human element are used to realize a given effect. He further discussed core strategies for combatting these asymmetric threats currently being considered by DoD, DHS, Congress, the Executive Branch, and across government and private industry.

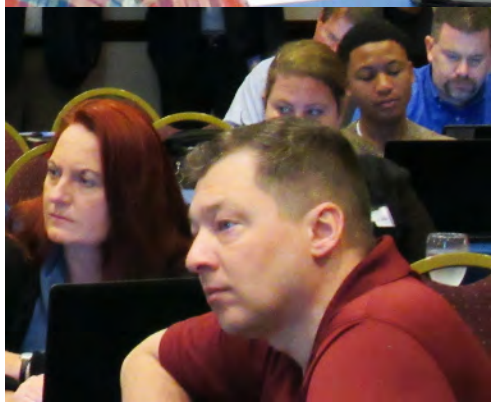
During the next session, Curricula's Nick Santora, examined how many organizations have security awareness programs but overlook the emotional intelligence behind their design. His session discussed various elements of awareness programs and how certain actions positively or negatively impact your employees and the security of your organization.

The workshop concluded with a presentation from DTE Energy reviewing the rationale and process DTE used to integrate risk into the development of standardized physical and electronic controls for Low Impact assets.

He discussed a process that began as a "one-size-fits-all" approach and developed into a risk targeted and standardized model resulting in new internal DTE impact ratings within the Low Impact rating of "Low-Minimum," "Low-Moderate," and "Low-Maximum."

The 2018 Fall workshop offered up a wide range of valuable information to the attendees and allowed for RF staff and ERO peers to connect.

Overall the workshop was a great success, and RF looks forward to your attendance at the 2019 Spring Workshop to be held at the Inner Harbor Baltimore during the last week of April 2019.



Upcoming Standards

To follow-up on our Workshop Presentation on Upcoming Standards, remember we will continue to use our Standards Page and our monthly CMEP Update Letter to keep you informed.

Also, you can always reference NERC's One-stop shop for Standards, implementation dates, and guidance/ guidelines in effect and the NERC list of Standards subject to future enforcement (use the drop-down to select Standards Subject to Future Enforcement).

- One Stop Shop
- Standards Summary

Fourth Annual Protection System & First Human Performance Workshop

RF hosted the fourth annual Protection System Workshop for Technical Personnel on August 14 and 15 at our Independence office and had more than 80 people in attendance, including speakers and vendors. The focus theme for this year was “Protection System Drawings - the Big Picture.” We want to thank everyone for taking the time to visit us and hope each attendee took away a few new tidbits to help with their everyday work!

A highlight of the workshop was a joint presentation given by ITC Transmission and Consumers Energy on the methods they have utilized in the past when interacting at shared substations and sharing drawings.

The workshop included a breakout session where attendees formed into small groups to discuss various issues and their current practicing or proposed solutions. This provided the opportunity for attendees to meet colleagues from other companies and talk about common issues and solutions. Groups could choose from a provided list of topics or any additional issue on system protection drawings. These included:

- Change management in the drawing process
- Whether to issue logic diagrams with drawings
- Large multistate project; how is it tracked and implemented
- Coordination on design details
- Dealing with multiple sets of prints

We appreciate the frank feedback that many of the attendees provided in their surveys on all aspects of the session. We are pleased that most attendees found the material useful and stated they would use it in their daily work. A

theme throughout the responses was how popular the breakout session item continues to be. Several attendees suggested adding more structure to this item and possibly reformatting it to include more time for discussion and having multiple people from each group report out to the audience. Incorporating additional personal experience stories and providing software solutions to the issues discussed were also suggested for future workshops.

Each year we try to make this workshop even better than the previous and the feedback received goes a long way to help improve the experience. Mark your calendars for next year’s workshop which is scheduled to be held on August 13-14, 2019. Thank you to all that attended and who continue to make this event a success. If you have questions, need more information, have topic suggestions or would like to present at future workshops, please contact John Idzior or Jeff Mitchell.

RF held its fourth annual Protection Systems Workshop for Technical Personnel and then immediately afterward, conducted its first Human Performance Workshop. The Human Performance Workshop focused on the practical application of human performance techniques and concepts for front-line activities that the attendees could take back and use in their work environments.

We had some very dynamic speakers to keep the audience engaged and to provide some practical principles and concepts of human performance. Survey comments were quite positive, and RF is considering conducting another human performance workshop in 2019. More information will be coming in future newsletters and on our website.

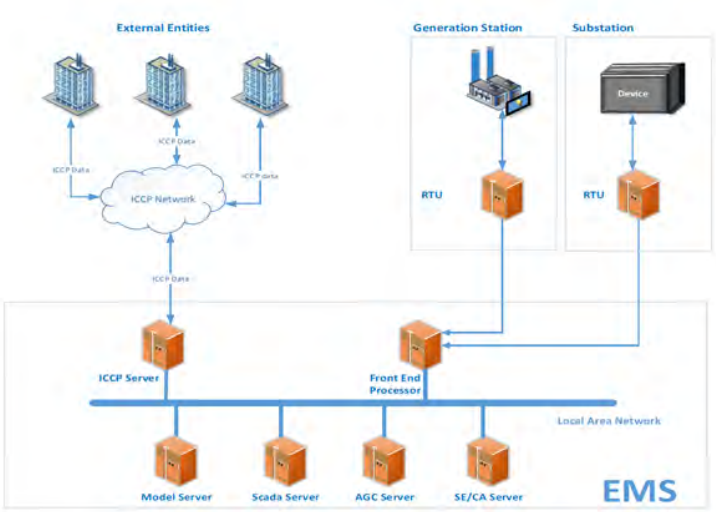
2018 Monitoring and Situational Awareness Conference

From October 2nd – 3rd, the RF Events Analysis and Situational Awareness (EASA) team attended NERC's ***Sixth Annual Monitoring and Situational Awareness Conference***, hosted by MISO. The theme of the conference was, "The Evolution of EMS Systems." The RF region was well represented at the conference with presentations by AEP, MISO, PJM, and Atlantic City/Delmarva. Highlights of the conference included presentations regarding:

- Incorporating voltage and transient stability tools into EMS systems
- Protecting EMS systems from cyber-security risks
- Utilizing the Common Information Model (CIM) when sharing EMS models
- Standards focused on EMS security/reliability plus Real-time Assessments (TOP-001-4, TOP-010-1(i), and IRO-008-2)
- Recent Lessons Learned from EMS events

A special thank-you goes out to all RF members who attended the conference, plus MISO for hosting.

Slides from the presentation will be posted on NERC's website soon.



For more information on NERC Lessons Learned, generated from the Event Analysis Process, click here.

And finally, for more EMS information in general, check out RF's EMS Knowledge Center on our website.

Continuing Cold Weather Site Visits

RF has been performing Cold Weather Preparedness site visits since 2014. From 2014-2017 we have identified and communicated more than 57 best practices and 32 lessons learned. The program has already improved winter performance in our region, and we want to ensure that success continues.

We are continuing to ensure that generating facilities have made the necessary preparations for winter readiness. As done in the past, plant winterization surveys will be sent to new generating facilities, those facilities that have experienced first-time cold weather related issues and those that experienced repeat issues during the 2017-2018 winter period. GADS remains the basis for identifying those entities experiencing cold weather related issues which resulted in failure to start, derates or trips. Possible site visits may include generating facilities in Ohio, Pennsylvania and New Jersey.

A generic plant winterization survey will be sent to new generating facilities and those experiencing first-time cold weather related issues. Those entities which had already completed a plant winterization survey in the past will only be required to provide updates to their previous responses. In some cases in lieu of another site visit, the entity will be expected to provide documentation of corrective actions to prevent or minimize the reoccurrence of the cold weather related issue. If site visits are conducted, RF will attempt to coordinate these efforts with the associated plant staff commencing in early November with completion planned for mid-December.

Calendar of Events

Complete calendar of RF Upcoming Events is located on our Website:

Date	RF Coming Events	Location
November 19	Reliability and Compliance Open Forum Call	Conference Call
November 28	RF Q4 Board of Directors Committee Meetings	Washington, DC
November 29	RF Annual Meeting of Members & Q4 Board Meeting	Washington, DC
December 17	Reliability and Compliance Open Forum Call	Conference Call

Industry Events:

Date	RF Coming Events
October 23-24	NERC Transmission Availability Data System Training
November 15	FERC Open Meeting
December 4-6	FERC Environmental Review and Compliance for Natural Gas Facilities Seminar
December 20	FERC Open Meeting

What's Happening in Illinois
NextGrid: Illinois Utility of the Future Study

In September 2018, NextGrid Illinois held meetings to discuss the future of Illinois utilities and to discuss the NextGrid draft report.

During the meeting, they discussed the current and emerging trends in distributed energy resources (DER) as well as startup companies that are paving the way for DER integration and emerging, innovative technologies.

Further, emerging trends and technologies on the grid were discussed as well as the challenges and opportunities of modernizing the grid. Discussion around the potential benefits of the future grid including increases in customer satisfaction, control, and convenience, as well as environmental benefits.

To view video of the meeting click here.

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