Issue 2
2020 March/April

INSIDE THIS ISSUE

Continuous Improvement	2-3
Oil and Gas Pipeline Security	4-5
Internal Controls Workshop	6
Get Control of Yourself	7-8
The Lighthouse	9-10
Regulatory Affairs	11
Standards	12-13
Watt's Up	14-18
Calendar	19
RF Members	20

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'd like to start by sending my heartfelt thanks to each and every one of the people working to keep the electric grid safe and reliable during the coronavirus outbreak. Your efforts play an integral role in helping our country make it through this trying time, so please know that the whole RF team and I are here to support you. The grid is the backbone of our economy, critical for our national security, and necessary to support public welfare—and I'm more proud than ever to be a part of this industry.

This newsletter is much like our work right now: a balance between addressing the unprecedented emergency affecting nearly every aspect of our lives, and not losing sight of the imperative work we do on a daily basis to ensure the lights are on today and will stay on tomorrow. Some content pertains to how we are responding as an industry, including guidance from NERC and FERC, and some is more typical of a newsletter during "normal" times. This mix of information was done purposely, and it exemplifies what I believe will become our "new normal" going forward. Remaining agile and aware will allow our focus on mitigating COVID-19 impacts to seamlessly complement and enhance our existing plans and activities to make us even more resilient.

RF's Business Continuity Plan was instituted in early March and included a mandatory work-from-home plan for all employees, as well as either canceling or switching all upcoming in-person meetings and events to web/video format. Decisions like canceling our much-anticipated Spring CIP and Reliability Workshop in Detroit are not taken lightly, but our top priority is the health and safety of all personnel at RF, our entities, stakeholders, and colleagues across the ERO Enterprise.

In line with the combination of content in this issue, we are recognizing personnel changes that are both happy and sad. This month, we happily welcomed Niki Schaefer back to RF as VP and General Counsel. Niki joining the team allows Rob Eckenrod to focus on his impactful new role of VP, Entity Engagement and Corporate Services.

It's with mixed emotions that I share the news that RF's Senior VP and Treasurer, Ray Palmieri, will be retiring, effective June 1. After nearly 50 years of service to the industry, I know many of you have had the distinct pleasure of working with Ray—and if you've had the pleasure, I can safely assume you will miss him too because he has always been known for his positivity, leadership and comradery. His legacy, at RF and throughout the industry, is one that will be lasting for many years to come.

Be safe and be well.

Forward Together,

Tim

Continuous Improvement

By Erik Johnson, Director, Reliability Analysis, and Sam Ciccone, Senior Reliability Consultant

This new column will be an ongoing series that will provide Continuous Improvement (CI) approaches to topics either discussed in other newsletter articles or any other topics deemed applicable to improving the Security, Resilience and Reliability of the grid.

"Without continual growth and progress, such words as improvement, achievement, and success have no meaning."
- Benjamin Franklin

This introductory article will discuss Continuous Improvement (CI) regarding the ever changing landscape of the NERC Reliability Standards.

You've made it through an audit with no Potential Non-Compliances (PNCs)…that's great, but you're journey has just begun!

What do we mean by your journey has just begun? In other words, by focusing only on compliance, you are only meeting a part of the challenge – and that is with no PNCs. Think of it like an oil pan and the oil that lubricates the engine; remove one and neither has much value. Another example is having a circuit breaker with no line attached. Breakers and lines are both integral to the grid, but one without the other has diminished value.

A last example for those military folks reading is protecting the rear of your forward force but not having a point person performing reconnaissance.

These examples illustrate the point that each part has equal value when they are together. A compliance program and a CI program have the same relationship – while only one is required, it takes both to address the Security, Resilience and Reliability of the grid.

The Journey to Security, Resilience and Reliability

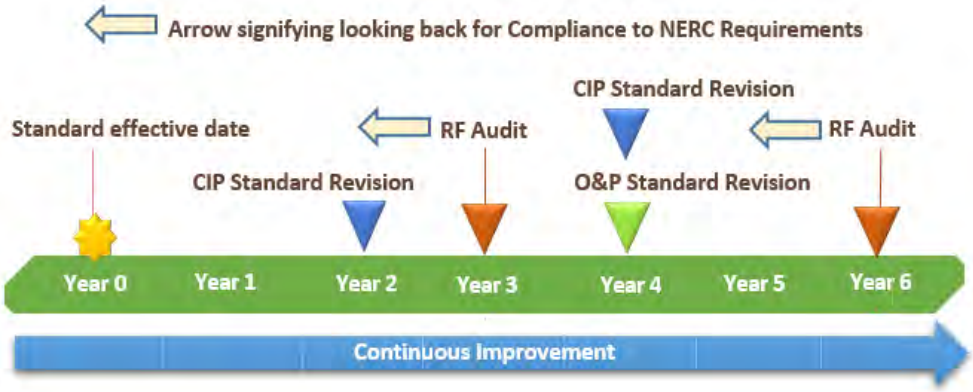
Wait a minute…shouldn't they write additional Standards if they want me to do more?

Yes and they are! Let's look at the impact of Standards duration and how CI prepares you for what's coming. NERC Compliance is sometimes a challenging and resource intensive process that also has moving targets in new and changing Requirements. For instance, here are some statistics about Standards revisions: Ops and Planning and CIP Standards have undergone major* revisions since FERC Order 693 (OPS/PLN) was released in 2007 and FERC Order 706 (CIP) was released in 2008. When you review the frequency of these revisions, on average, NERC Standards have been revised every four years (O&P) and every two years (CIP).

You'll notice this graphical timeline below the view of Standard revisions and audits includes the proposed CI program discussed in this article.

What Does This Mean?

Changing Standards and having to implement new (or retool existing) processes as a result of new and changing Requirements adds to the complexity of entity compliance and audit preparations. Although this is a Compliance Specialist's full-time job, the scope often falls short of including a focus on CI. Looking ahead to changes, instead of reacting to them as they come, can be instrumental to success. Many entities are required to look back three years for each audit scheduled and performed by RF.



Continued on page 3

Continuous Improvement

Continued from page 2

Some entities are on a six-year cycle, and this could mean multiple Requirement changes, especially on the CIP side. During that time, the entity needs preparation for possible new Requirements. This takes proper planning and having effective processes in place to be efficient and successful – not only for compliance, but for organizational maturity, as well as Security, Resilience and Reliability.

What Is the Solution?

What if before, during and after your audit you are looking forward for CI opportunities that you can quickly, efficiently and cost effectively implement? Could this lead to better compliance results that facilitate the creation of programs that build mature and resilient processes that, in turn, increase organizational and compliance program maturity? We believe it can, but there are challenges:

- **Competing Values**: As stated by Rony Kubat in a 2019 article, "compliance and continuous improvement evince fundamentally different values: change vs. consistency. Progress vs. stasis. Risk ready vs. risk averse. Frame it how you will, but there are good reasons manufacturers find themselves on one or the other side of the divide."[1]

- **Management Buy-In**: Possibly the most important part of developing and implementing improvement activities is complete buy-in from top management. Management must be convinced that these activities will reduce resource intensity and help the organization achieve its goals. Furthermore, management needs to see measurable results from the CI program. Without this dedication from the top, the CI program cannot be implemented, or at best it will be implemented inconsistently among areas of the organization that choose to develop their own CI program.

Where Do I Begin?

There are many ways to begin a CI program. Here are a few ideas:

- Participate on a NERC Standards Development Team or comment on Standards that are being developed; this will keep your organization in tune with developments that will impact it.

- Implement tracking metrics to identify and group problem areas and areas where things are performing as expected. This will allow for focusing on areas that need improvement and learning from areas that do not.

- Use the RF Assist Visit program, North American Transmission Forum (NATF) and North American Generator Forum (NAGF) reviews to strengthen processes and procedures.

- Utilize the RF Cyber Resilience Assessment Tool or Continuous Improvement self-assessment.

How Can RF Help?

Assessments can provide a clear and quantitative snapshot of your current state of organizational and compliance program maturity. The RF Entity Development department provides this service, and entities are encouraged to contact RF for an overview of the process. We can evaluate the current state of your reliability maturity by utilizing a model that was built for and tailored to the electric utility industry, as well as providing entities with the ability and intuitive tools to perform these assessments on their own.

Regardless of the method, these assessments generate a roadmap for your CI program. Follow-up status touchpoints and guidance from RF on this roadmap can help an entity show results to their top management. Furthermore, follow-up assessments can also provide benefits by reducing specific risks the entities are facing.

[1] Balancing Compliance and Continuous Improvement in Highly Regulated Industries

*Major revisions do not include interpretations added to the Standards or errata changes made to the Standard.

Oil and Gas Pipeline Security

By Tony Freeman, Principal Analyst, Risk Analysis and Mitigation

Transportation Security Administration

Last year's ransomware attack causing a two-day pipeline shut down for a natural gas supplier, as well as a 2018 incident causing Transportation Security Administration (TSA) communication channels to go down, have sparked ongoing controversy regarding the safety and security of oil and natural gas pipelines. These events raised questions about the amount of resources dedicated to physical and cybersecurity for these pipelines.

With nearly 1,800 natural gas powered generation facilities across North America, they are responsible for producing nearly 34% of our nation's electricity, according to statistics from 2018.

Outside of power generation, we must also mention other commercial uses for natural gas in the creation of antifreezes, plastics, pharmaceuticals and fabrics, and our home-life dependencies on natural gas such as heating, cooking, etc. We can reasonably ascertain from these uses that even the smallest attack on the gas industry pipelines would be detrimental to U.S. businesses and citizens.

The Federal Energy Regulatory Commission (FERC) has raised a number of concerns regarding the security of these nearly 2.7 million miles of U.S. pipeline. A primary concern is the TSA's pipeline branch staffing levels, which have fluctuated between only one and six personnel from 2014 through 2018.

A secondary concern is the lack of cyber security expertise within this workforce. Other FERC concerns include the lack of mandatory compliance obligations and cyber security reporting requirements. The TSA primarily relies upon internal self-reporting of cyber security incidents by pipeline infrastructure operators in order to identify, track and/or correct security issues.

The TSA, as well as other government agencies, are working to improve the security and safety of these pipelines and to ensure there is no interruption of natural gas and oil supply. In an ongoing effort to share data, more than 50 U.S. gas and oil companies utilize the Oil and Natural Gas Information Sharing and Analysis Center (ONG-ISAC) to share cyber-threat and physical security intelligence amongst themselves and the federal government.

These efforts come at a time in which the attacks are growing in complexity, now targeting Operational Technology (OT) networks where historically they were focused on IT networks.

The TSA has released its own Pipeline Security Guidelines that further expand on their efforts to increase the security posture of this infrastructure. Just as in the power industry, the TSA is striving to achieve a risk-based approach and applying it to security, as outlined in the Department of Homeland Security's (DHS) National Infrastructure Protection Plan (NIPP). Following the NIPP model, the TSA has outlined four key categories in achieving a positive security posture through risk analysis: Criticality Assessment, Facility Security Measures, Pipeline cyber asset security measures, and protective measures for the National Terrorism Advisory System (NTAS) alerts.

Similar to the NERC CIP-002-5.1a R1 regulatory Standard, TSA has implemented a guideline for pipeline facility criticality assessments to not exceed an 18-month window. This assessment includes documenting the methodology utilized in determining the criticality of a particular facility, securing and maintaining a list of the company's critical facilities, as well as conducting a Security Vulnerability Assessment (SVA).

The SVA is to be conducted at least every 36 months, or 12 months in the event of significant enhancements or site modification.

Continued on page 5

Oil and Gas Pipeline Security

Continued from page 4

A facility is deemed critical based on its potential impact if destroyed or downgraded, and the determining criteria include the potential to cause:

- Disruption or delivery to installations identified as critical to national defense;
- Economic disruptions, including the disruption of services to power plants and major airports;
- A mass casualty situation;
- Disruption of a service that would adversely impact a state or local government from providing essential public services and emergency response;
- Damage to national landmarks or monuments;
- Negative impacts to major waterways or public drinking water supplies;
- Negative impacts to home/consumer delivery for an extended period of time; or
- Negative impacts or disruption to system operation/business of critical facilities.

Site specific/Facility Security measures are to be reviewed every 18 months and must be tailored to the NTAS Bulletins/Alerts. Regardless of the criticality level, the TSA has implemented guidelines advising oil and gas companies to baseline their security measures, as well as baselining the enhanced security measures at critical facilities.

The TSA's Cyber Security Measures for Cyber Asset Classification can be divided into two categories: OT systems responsible for the control of the pipeline and non-critical pipeline assets, which are those OT systems are used for monitoring purposes. Some of the cyber security measures should look familiar and include, but are not limited to, the following measures alongside the similar NERC CIP-related counterpart:

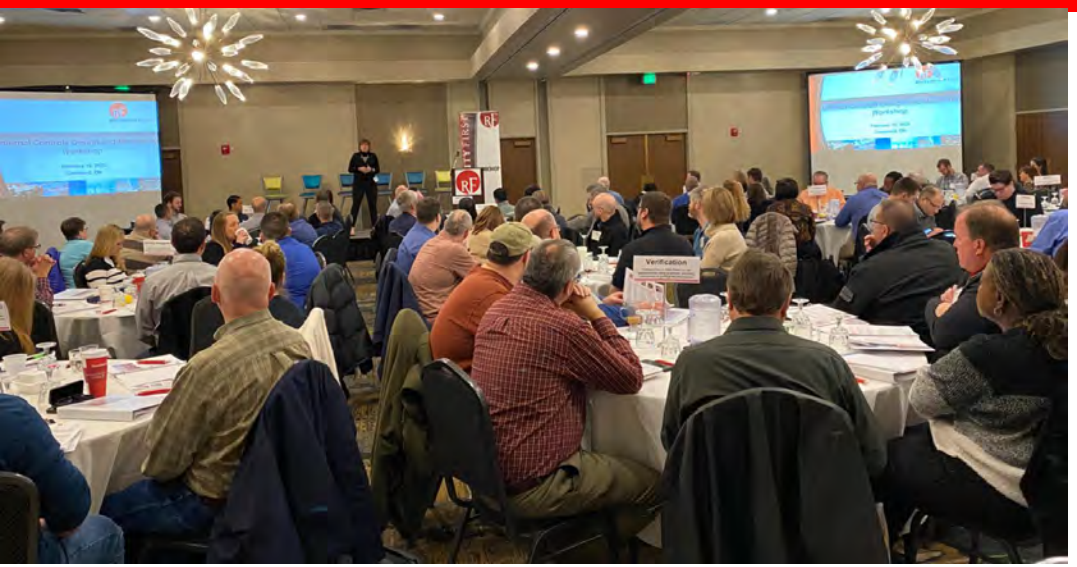
- Establishing procedures and policies for configuration change management to ensure that no changes adversely affect cybersecurity controls (CIP-010-2)
- Maintaining Network/system architecture diagrams
- Review of Cyber Security Policies every 36 months (CIP-003-6)
- Establishing a process to identify and evaluate vulnerabilities and compensatory measures (CIP-002-5.1a & CIP-010-2)
- Access requires Cyber Security Training (CIP-004-6)
- Identification of critical data (CIP-011-2)
- Logging and alerting (CIP-007-6)
- Monitoring for unauthorized access (CIP-004-6)
- Response Planning and Disaster Recovery (CIP-008-5)

Though these practices are being implemented, a completion date for all of these items is yet to be determined, leaving potential risk exposure from a vendor and dependency perspective.

For additional information and the formal report provided by the Government Accountability Office please utilize the following link: GAO Report to Congressional Requesters: TSA Pipeline Security Program Management.

If you have any additional questions, comments or concerns regarding Risk Analysis, Mitigations or Evidence please feel free to contact the Reliability First Risk Analysis and Mitigation (RAM) department via our Contact Us page, and be sure to select "Risk Analysis & Mitigation" from the list of Areas.

First Internal Controls Workshop a Success



ReliabilityFirst held its first Internal Controls Workshop this February in Cleveland, OH. More than 120 Subject Mater Experts (SME) and Primary Compliance Contacts (PCC) from 53 different Entities attended the event, as well as individuals from four Regional Entities, NERC and FERC.

The one-day workshop consisted of presentations from RF internal controls SME and Principal Technical Auditor Denise Hunter, presentations from various Entities addressing internal controls at their respective organizations, a panel discussion, and an afternoon working session.

The day began by introducing an internal control framework based off the Committee of Sponsoring Organizations' (COSO) that can be used to help Entities frame their internal controls and programs. RF offered instructions for writing internal controls, shared three different templates entities can use to capture their controls, and provided examples of documented internal controls for PRC-004-5(i) and CIP-007-6 R2, as well as internal control flashcards. Representatives from three Entities presented their programs addressing PRC-004-5(i) and CIP-007-6 R2 and detailed how they have implemented internal controls into their procedures.

This was followed by a panel discussion where they shared their experiences with identifying, designing and implementing internal controls in their environment and the challenges they encountered. This was vital to the success of the workshop, as other Entities were able to ask questions and solicit feedback from individuals who have gone through this process at their organization.

To enhance engagement at the workshop, RF implemented a few innovative concepts. The concepts included: seating based on Entity risk to ensure relevant discussions during the afternoon working session, providing hard-copy workbooks, restricting laptop use, and providing the frameworks and templates as options for Entity use. These new ideas resulted in a workshop that was engaging and interactive, and it cultivated a collaborative work environment by removing distractions and placing Entities together with others that were facing the same risks and most likely dealing with similar internal issues.

The great deal of participant feedback is much appreciated by the RF team, and it will be taken into consideration as we begin to plan for the next Internal Controls Workshop. The goal for all RF workshops is for the Entities to learn and interact with each other, so gaining insightful feedback from the community allows us to ensure we are providing what the Entities in our footprint want and need.

Please keep an eye out for information about the next one, and thank you to everyone who was involved in making this first workshop a success.

Get Control of Yourself - Risk Moves Pretty Fast

By Denise Hunter, Principal Technical Auditor

It was incredibly difficult figuring out how to start this article. In a time when coronavirus concerns outweigh practically everything, some might think this is not the time to discuss internal controls.

However, watching our industry leaders proactively address this situation has been a good reminder that a properly aligned internal control program can help entities respond to the risks they are facing. Times like these can show how your internal control program flexes and retracts, and this can help you reassess, address and mitigate the risks at hand.

Ferris Bueller said, "Life moves pretty fast. If you don't stop and look around once in a while, you could miss it." I would change that to: "Risk moves pretty fast." The front page of "USA Today" on January 27 discussed how the coronavirus had spread through China. At that time, the U.S. had diagnosed five people with the virus. Fast forward a mere three months, and we are in the middle of a pandemic. Risk can move fast.

The nature of our business ensures that we plan. It is likely that one of the controls you have implemented due to the pandemic is a Business Continuity Plan (BCP). Among the various activities that could be included in a BCP, it usually includes a Disaster Recovery plan, a Contingency plan, and a Crisis Management plan.

A Crisis Management plan is a reactive control consisting of an underlying framework that, at a minimum, should identify:

1) What the organization identifies as a crisis. This should include the criteria to determine a crisis and an outline of the initial steps to take for each type of crisis identified. It should provide enough information to allow for the determination of when to escalate the plan and should be scalable to fit each event.

2) An established crisis management team that includes representation from each key department. These personnel should be aware of the expected "must do" tasks for their department.

3) Established communication networks, including details for what information to communicate, how to communicate it, and to whom. This could include personnel who are not normally included in day-to-day operations; therefore, consideration must be made to ensure that this information is current and accurate.

4) A resource library of any key documentation that could be critical during a time of high stress (i.e., checklists, one line drawings, etc.).

The amount of details you may have had to address during this unprecedented event depends largely on how much your existing plans contemplated pandemics. However, the process to determine which internal controls you should add has remained the same. First, you had to identify your risk.

What was the initial risk? It was that control center and field personnel could be compromised and not available to perform their duties. We learned from the Centers for Disease Control and Prevention (CDC) that the virus spreads through respiratory droplets from an infected person. Alternatively, it might spread through touching your face, eyes, nose or mouth after coming in contact with a surface that has the virus on it.

Therefore, based on the CDC and possibly the Electricity Subsector Coordinating Council recommendations[1], you may have implemented some (or all) of the following control activities.

a) To reduce the possibility of transmission between employees, you may have: encouraged sick employees to stay home,

[1] Electricity Subsector Coordinating Council - Assessing and Mitigating the Novel Coronavirus (COVID-19) https://www.cdc.gov/coronavirus/2019-ncov/prevent-getting-sick/prevention.html

Continued on page 8

Get Control of Yourself - Risk Moves Pretty Fast

Continued from page 7

established a process to ensure prompt notification of changes, educated employees on steps to protect themselves and reduce spreading the virus, and identified that sharing phones and other equipment should be avoided.

b) To ensure critical grid operations are maintained, you may have: identified a point person responsible for COVID-19 issues and their impact, talked with your vendors to determine the control activities they are performing to ensure they meet your established guidelines, maintained contact with suppliers to determine if they are having issues in order to implement back-up supplier procedures, and considered contacting neighboring entities to establish back-up capabilities.

c) To maintain a safe work environment, you may have: identified ways to increase ventilation within the facility, established a routine to perform disinfecting of frequently-touched workstations/surfaces, and put up signs to remind employee to wash their hands and clean their areas. You also may have set reminders for these control activities, considering they are not normally performed during each shift.

Now that you have established the appropriate controls, we are finished. Right? Actually, the hard part is just beginning because none of these controls are commonplace. We share items like phones and workstations on a daily basis and often without a second thought.

Now, add to these habits that it is human nature to be distracted and revert back to previous activities in times of high stress. Plus, our governments are starting to talk about loosening some restrictions. So, do we really need to continue these controls? The CDC would say, Yes!

So how do we continue to mitigate this risk? If you had the opportunity to attend the RF Internal Controls Workshop in February, you know that this is when the importance of monitoring begins. This includes checklists, sign-off sheets and whatever controls you deem necessary to ensure that what you want to happen, consistently continues to happen.

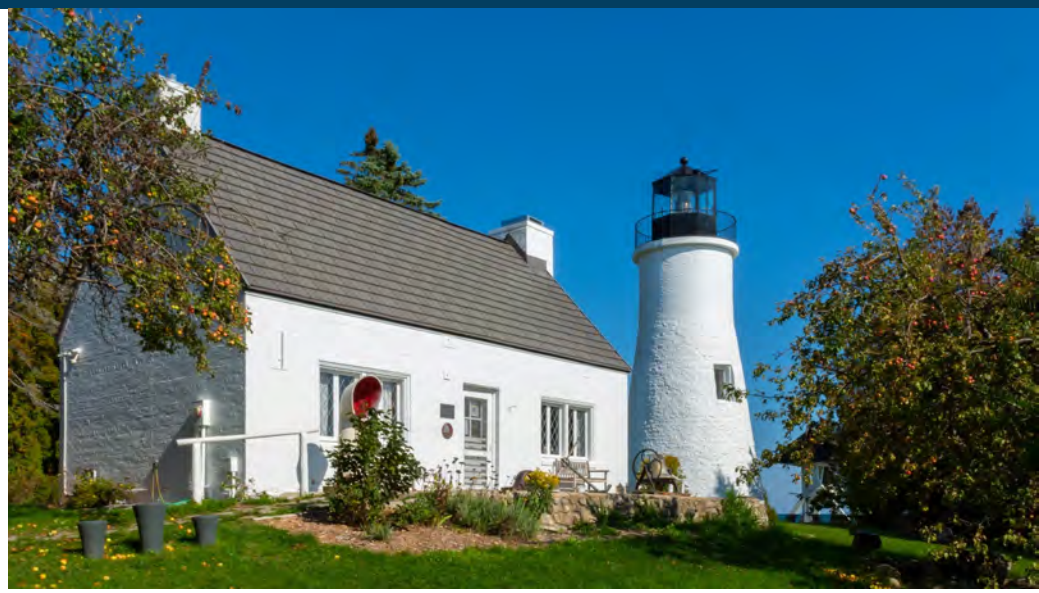
If ever the importance of departmental monitoring was apparent, that time is now. We have been raising the conversation regarding controls outside of Standards. No Standard addresses this huge risk.

Risk can move fast. With the correct control framework in place and the understanding that we must remain agile in order to address the appropriate risk at the correct time, we will get through this. The time and effort that has been put into our control programs should, and will, assist you in responding to these events.

We'll talk again soon. Until then, stay safe and healthy.

By Lew Folkerth, Principal Reliability Consultant

Foundations - Part 1



Old Presque Isle Lighthouse, Presque Isle, MI – Photo: L Folkerth

In this recurring column, I explore various questions and concerns related to the NERC Critical Infrastructure Protection (CIP) Standards. I share my views and opinions with you, which are not binding. Rather, this information is intended to provoke discussion within your entity.

It may also help you and your entity as you strive to improve your compliance posture and work toward continuous improvement in the reliability, security, resiliency and sustainability of your CIP compliance programs.

There are times that I also may discuss areas of the Standards that other entities may be struggling with and share my ideas to overcome their known issues. As with lighthouses, I can't steer your ship for you, but perhaps I can help shed light on the sometimes stormy waters of CIP compliance.

I've had some discussions recently that point out how much background is needed to be proficient in the CIP Standards. I think it's time to look at what all CIP professionals should have in their toolbox. Some may need more depth in certain areas, but the foundations of CIP should be fairly constant across all professionals. I don't advocate memorizing the Standards or other documents, but you should know where to find the essential documents and where to find the appropriate information within those documents.

For the purposes of this article, I'll assume you're new to the CIP Standards, but this material should be useful to all CIP professionals, even if only as a review.

Understand Our Industry

In order to identify and protect the appropriate equipment and supporting systems, you should have a basic understanding of the electric industry and how it works. The electric industry is engaged in the generation, transmission and distribution of electric power.

To have the proper context in which to understand the CIP Standards, you should understand the industry's fundamentals and the associated terminology.

Our industry is based on electricity, in particular alternating current. You should understand the difference between electric potential, measured in volts and sometimes called "voltage," and electric current, measured in amperes or amps. You should understand the difference between real power, measured in watts; reactive power, measured in vars; and energy, measured in watt hours.

Generation is the process of taking energy in one form, such as heat, and turning it into electrical energy. **Transmission** moves the electrical energy from where it's produced (generation), to near where it's needed. **Distribution** takes electric energy from transmission and moves it to where it's finally used, known as "demand" or "load."

Generation of electric energy must match – on a moment-to-moment basis – the demand for electric energy.

As the demand for electric energy changes, generation must be adjusted to match so that neither too much nor too little energy is available at any time. This is known as "balancing" and is a critical process in the electric industry.

Understand the Role of Compliance in Our Industry

Priorities

As part of the electric industry, you must be aware of the proper place of compliance within the overall picture of the industry.

Continued on page 10

Continued from page 9

Electric Industry Priorities

1. **Safety**
2. **Reliability**
3. **Compliance**

The first priority is the **safety** of electrical employees and the general public. The second priority is **reliability**, "keeping the lights on." Security, both physical and cyber, is considered to be part of reliability.

The third priority is **compliance**. The purpose of the CIP Standards is to improve reliability by keeping the equipment essential to reliability secure. The concept of CIP Exceptional Circumstances written into the CIP Standards is an acknowledgment of this fact.

Risk

Regulators and industry are coming to understand that the role of compliance is to manage and reduce risks to reliability. One of our newest Standards, CIP-013-1, Supply Chain Risk Management, is explicitly written to require risk to be managed. You should be familiar with risk management methods and risk assessments.

Understand Our Essential Documents and How to Read Them

Standards

In order to understand the CIP Standards, we need to understand the documents governing these Standards. First and foremost are the Standards themselves, but you need to know how to read them.

The NERC Reliability Standards, of which the CIP Standards are a part, are created according to the Standard Processes Manual. You should at least review this manual, which is Appendix 3A to the NERC Rules of Procedure, but carefully read Section 2.5.

The last paragraph of this Section tells us that the only mandatory and enforceable parts of a Standard are the applicability, the effective dates, and the Requirements.

In addition to these three enforceable components of the Standards, defined terms may be developed and approved for use in the Standards. These defined terms, once approved, appear in "Glossary of Terms Used in NERC Reliability Standards" (NERC Glossary) and are an officially recognized component of the Standards.

A Standard may also have an accompanying implementation plan containing effective dates and other information, such as initial performance of periodic Requirements. Implementation plans are approved as part of the Standard and are also enforceable.

All other parts of a Standard are considered guidance and may not be directly enforced. This guidance can help in understanding the Standard, but it cannot override the language of a Requirement.

For example, if a statement in the Measures section of a Standard conflicts with the language of a Requirement, the language of the Requirement prevails.

Guidance

The NERC Guidance Policy defines two types of approved guidance documents: Implementation Guidance and Compliance Monitoring and Enforcement Program (CMEP) Practice Guides.

Implementation Guidance is developed by industry and approved for adoption by the ERO. It provides examples of how a Standard or Requirement might be implemented.

CMEP Practice Guides are instructions for auditors and other CMEP staff to consider when assessing compliance to a Standard. They are developed by the ERO Enterprise and posted publicly.

Guidelines

Guidelines are developed by one or more NERC standing committees and are posted to the NERC website. Guidelines provide recommendations on how to improve or maintain the reliability of the BES. Although they are not enforceable, industry is encouraged to understand and follow them.

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.

Feedback

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

Lew Folkerth, Principal Reliability Consultant, can be reached here.

Regulatory Affairs

FERC Issues Notice of Inquiry Regarding Virtualization and Cloud-Computing Services

On February 20, FERC issued a Notice of Inquiry (NOI) that seeks comments on potential benefits and risks associated with the use of virtualization and cloud computing services in BES operations. It also examines whether barriers exist in the CIP Standards that impede the adoption of virtualization or cloud computing services.

The NOI came in response to discussions on these topics at FERC's 2019 Reliability Technical Conference and the 2019 FERC/DOE Security Investments for Energy Infrastructure Technical Conference. FERC is determining whether it would be appropriate to direct that NERC develop modifications to the CIP Reliability Standards to facilitate the voluntary adoption of virtualization and cloud computing services by registered entities.

The NOI is seeking comment in four areas:

(1) the scope of the potential use of virtualization and cloud-computing services;

(2) the potential benefits and risks associated with virtualization and cloud-computing services;

(3) the potential impediments to adopting virtualization and cloud-computing technologies; and

(4) the potential use of new and emerging technologies, other than virtualization and cloud-computing services, in the current CIP standards framework.

FERC and NERC Take Early Steps to Address Reliability amidst COVID-19

On March 18, FERC and NERC published guidance on how to ensure grid reliability in the face of the changes and impacts that COVID-19 has brought to the industry. On April 2, NERC released an FAQ document to provide clarification regarding some of the changes, and they will regularly update the document as new questions are received.

The major considerations FERC and NERC announced in their initial guidance are:

- **Personnel Certification:** The effects of the coronavirus will be considered an acceptable basis for non-compliance with obtaining and maintaining personnel certification, as required by PER-003-2, for the period of March 1, 2020 to December 31, 2020.

- **Standards involving Periodic Actions:** The effects of the coronavirus will be considered an acceptable reason for case-by-case non-compliance with Reliability Standard requirements involving periodic actions that would have been taken between March 1, 2020 and July 31, 2020. Examples include timing requirements under PRC-005-6 and CIP-007-6 R2.

RF issued instructions that in case of delay in compliance activities under either of the two scenarios described above (PER-003-2 or Standards involving periodic actions), entities should notify RF of their exception request using RF's Exception Request Form, available here. Entities should communicate and document the following information.

- What specific Standard/Requirement is at issue?
- What circumstances exist at your entity relating to COVID-19 that will prevent the compliance activity from being completed on-time?
- Are there interim mitigating activities you are putting in place?
- What actions will you need to take to get back into compliance, and when do you anticipate that these will be complete?

NERC's FAQ document made clear that any dates associated with these changes are subject to change as circumstances continue to develop around COVID-19. Further, the common theme throughout the FAQs was that responsible entities should communicate their COVID-19-related issues with their Regional Entity as quickly and clearly as possible. And while the initial guidance indicated that non-compliance with periodic actions would be acceptable on a case-by-case basis, non-compliance with non-periodic actions, even those that resulted from COVID-19, are still a basis for submitting a self-report.

In addition to the jointly-published guidance on grid reliability, NERC filed a motion with FERC to defer the implementation of seven new or updated Reliability Standards that were set to go into effect in the coming months. On April 17, 2020, FERC issued an Order granting this motion, with a three-month deferral of the implementation of CIP-005-6 (Cyber Security – Electronic Security Perimeter(s)), CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments), and CIP-013-1 (Cyber Security – Supply Chain Risk Management); and a six-month deferral of the implementation of PRC-002-2 (Disturbance Monitoring and Reporting Requirements), PRC-025-2 (Generator Relay Loadability), PRC-027-1 (Coordination of Protection Systems for Performance During Faults), and PER-006-1 (Specific Training for Personnel).

Standards Update

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

General NERC Standards News

FERC/NERC COVID-19 Specific Standards Guidance

On March 18, 2020, FERC and NERC collaborated on "Industry Guidance to Ensure Grid Reliability Amid Potential Coronavirus Impacts." This document includes two areas where FERC and NERC will consider the impacts of Coronavirus as a basis for noncompliance:

- The effects of the coronavirus will be considered an acceptable basis for non-compliance with obtaining and maintaining personnel certification, as required in Reliability Standard PER-003-2, for the period of March 1, 2020 to December 31, 2020. Registered entities should notify their Regional Entities and Reliability Coordinators when using system operator personnel that are not NERC-certified.

- The effects of the coronavirus will be considered an acceptable reason for case-by-case non-compliance with Reliability Standard requirements involving **periodic actions** that would have been taken between March 1, 2020 and July 31, 2020. Registered entities should notify their Regional Entities of any periodic actions that will be missed during this period.

Other COVID Relevant Resources Posted

NERC/FERC have posted the following additional resources:

- In order to provide additional guidance regarding standards and compliance application resulting from COVID-19 NERC and FERC created a FAQ Spreadsheet about Joint NERC–FERC Industry Guidance for COVID-19.

Notable NERC Filings

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

- NERC filed a motion to FERC, to delay upcoming implementation deadlines of certain Reliability Standards in response to coronavirus-related disruptions.

- NERC requested the following implementation deferments:
  - Reliability Standard CIP-005-6 – Cyber Security – Electronic Security Perimeter(s), by three months;
  - Reliability Standard CIP-010-3 – Cyber Security – Configuration Change Management and Vulnerability Assessments, by three months;
  - Reliability Standard CIP-013-1 – Cyber Security – Supply Chain Risk Management, by three months;
  - Reliability Standard PER-006-1 – Specific Training for Personnel, by six months;
  - Reliability Standard PRC-002-2 – Disturbance Monitoring and Reporting Requirements (phased-in implementation for Requirements R2-R4 and R6-R11), by six months;
  - Reliability Standard PRC-025-2 – Generator Relay Loadability (phased-in implementation for Requirement R1, Attachment 1, Table 1 Relay Loadability Evaluation Criteria Options 5b, 14b, 15b, 16b), by six months; and
  - Reliability Standard PRC-027-1 - Coordination of Protection Systems for Performance During Faults, by six months.

- On April 17, 2020, FERC granted the above motion and deferments therein.

Standards Update

New Standards Projects

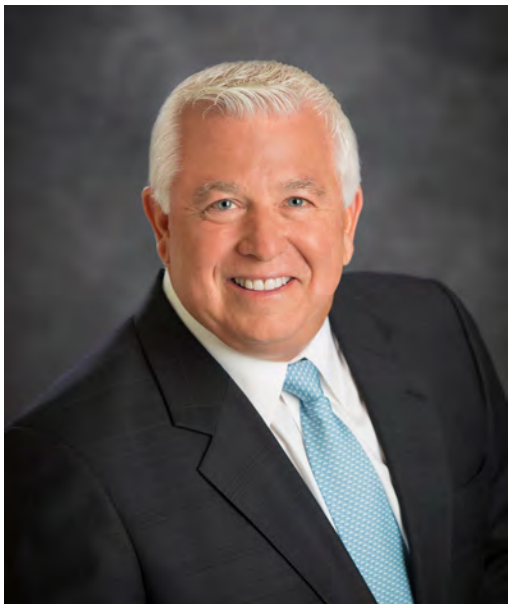
New Standards projects are described on the NERC Standards website, along with links to all drafts, voting results, and similar materials. Recent activity includes:

Project	Action	Start/End Date
Project 2020-03 - Cyber Security Supply Chain Low Impact Revisions	Comment Period	04/03/20 - 5/6/20
Project 2020-4 - Modifications to CIP-012	Comment Period	04/08/20 - 05/11/20
Other Active Comment Periods		
Comment Period Open for Distributed Energy Resources (DER) Data Collection for Modeling in Transmission Planning Studies Draft Reliability Guideline	Comment Period	3/11/20 - 4/24/20

Recent and Upcoming Standards Enforcement Dates (Please see notes in "Notable NERC Filings" section regarding the deferment of some of the below standards.)	
April 1, 2020	CIP-003-8 – Cyber Security – Security Management Controls
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.

RF Senior VP & Treasurer Ray Palmieri Retiring



Ray Palmieri, RF Senior Vice President and Treasurer, announced his retirement, effective June 1, 2020. In addition to serving as treasurer since 2012, Palmieri was a member of the team who established ReliabilityFirst Corporation in 2006, and he was the organization's sole vice president for many years before being promoted to senior vice president.

He was responsible for the leadership and implementation of the Reliability Engineering, IT and Finance functions, and he continued to support RF's efforts to ensure the NERC and RF policies, procedures and standards were adhered to such that reliability of the Bulk Power System was advanced.

"It would be difficult, if not impossible, to sum up Ray's immeasurable contributions to the industry and tireless efforts to advance RF," said Tim Gallagher, president and CEO. "I'm grateful to Ray for his partnership over the last 15 years in developing RF since its infancy to become the strong Region it is today, as well as for his friendship, leadership, comradery and passion for this industry. There are so many of us throughout the ERO who know Ray and have been touched by our interactions with him, and his legacy in our industry is one that will last for many years to come."

Palmieri's leadership elevated the importance of industry performance monitoring, and he championed enhanced performance and reliability management through feedback and a drive toward continuous improvement.

"Throughout my career, I'm fortunate to have connected and engaged with such talented and dedicated professionals, and I'm proud of the strides we made to advance the compliance aspects of the industry," said Palmieri. "Out of my many wonderful memories of RF, the most significant is the people — all brilliant, caring and always willing to help, but with a strong common mission of advancing the performance of the industry in any way they could. The success of the utility industry is paramount to the advancement of society, and I wish the industry and all the people in it nothing but success in carrying out the mission I've enjoyed working toward together for the past 47 years."

Prior to the establishment of RF, Palmieri worked in the ECAR region, starting up the compliance program for one of the three predecessor reliability regions that formed RF. He has worked with and chaired a number of NERC teams, including compliance, standards, registration, organization certification and reliability coordination. He held various senior leadership positions in Operations, Engineering and support functions for 24 years at the Nuclear Generation Facilities for Northeast Utilities and Exelon, as well as maintaining a Senior Reactor Operators license for 15 years.

Palmieri is a Professional Engineer in New York and Connecticut; a member of the American Society of Mechanical Engineers; a past chairman and member of various Nuclear Industry Owners Groups; and served as a Lieutenant in the U.S. Naval Reserve. He graduated from New York Maritime College with a Bachelor of Engineering in Marine/Mechanical Engineering and holds an MBA from Rensselaer Polytechnic Institute.

RF Welcomes Niki Schaefer as VP and General Counsel

ReliabilityFirst is pleased to welcome Niki Schaefer back to the organization. As Vice President and General Counsel for RF, Schaefer is responsible for ensuring the Compliance Monitoring and Enforcement Program (CMEP) functions are effectively executed for electric utilities in the 13 states and Washington, D.C. that make up the RF footprint. In this role, she leads the Legal, Enforcement and Compliance Monitoring teams.

"Niki's extensive background in helping shape strategic objectives and policies, as well as managing high-performing teams, make her uniquely positioned to significantly contribute to RF's mission of preserving and enhancing the reliability and security of the bulk power system," said Tim Gallagher, president and CEO. "Those who had the pleasure of working with Niki during her previous time at RF understand why we are so thrilled to welcome her back to the team."

As part of RF's ongoing efforts to serve entities and stakeholders more effectively, Rob Eckenrod will take on the new role of Vice President, Entity Engagement and Corporate Services.

"Rob has been an outstanding addition to the RF team, and this new role marries his comprehensive experience on 'the other side of the table' with the knowledge he's gained as a key leader at RF this past year to deliver proactive solutions to our industry partners," said Gallagher. "We recognize that COVID-19 has created challenging times for everyone but the organizational changes better position RF to meet the needs of our constituents, and given our history with both Rob and Niki, we have every confidence in their ability to help lead us through it."

Schaefer returns to RF from Eaton Corporation where she served as counsel to senior leadership teams across multiple business units within Eaton's Electrical Sector supporting more than $2 billion in revenue. Prior to Eaton, she was the Managing Enforcement Counsel at RF and directed the teams responsible for carrying out enforcement of electric reliability regulations. Before working in the electric industry, she was a trial lawyer for a large Cleveland law firm litigating commercial and personal injury cases in State and Federal Courts across the country.

Schaefer received her B.A. in American Studies from Cornell University and graduated cum laude from Case Western Reserve University School of Law where she received an academic scholarship.

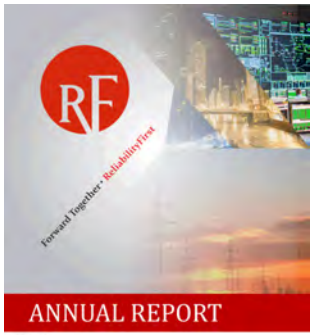
In addition to earning multiple professional awards – most recently being named to the 2020 Super Lawyers list by Cleveland Jewish News – Schaefer is very active in the Cleveland community through volunteer work for University Hospitals Partnership for Families and the American Heart Association. She is also a member of the Board of Directors of The Gathering Place, a non-profit that provides free therapeutic services to people with cancer and their loved ones.

RF Establishes Vegetation Management Group

ReliabilityFirst is forming a Community of Practice (CoP) for vegetation management personnel. A CoP is a group of people who share an interest or a passion for something and want to learn how to do it better through interacting regularly with other colleagues in that field of expertise. This is an informal gathering of vegetation management experts to debate current issues, share lessons learned, and discuss success stories and/or near-misses in a confidential, technical environment. This group is voluntary and available at no cost.

Vegetation management professionals, if interested, should reach out to Thomas Teafatiller, Principal Engineer - Protection, to receive more information about this new initiative.

RF Publishes 2019 Annual Report



The 2019 Annual Report describes ReliabilityFirst's activities in risk identification and mitigation, including prioritizing risks in our footprint and working with entities to ensure mitigation, as well as communicating risks and mitigation strategies to the ERO Enterprise and across our footprint. These activities are central to our mission of preserving and enhancing the reliability and security of the bulk power system.

The Report also highlights the RF Innovation Awards and Retreat; the new Cyber Resilience Assessment Tool; GridEx V; and provides trending and metrics on the latest risks and compliance challenges facing the industry.

Click here to access the Annual Report.

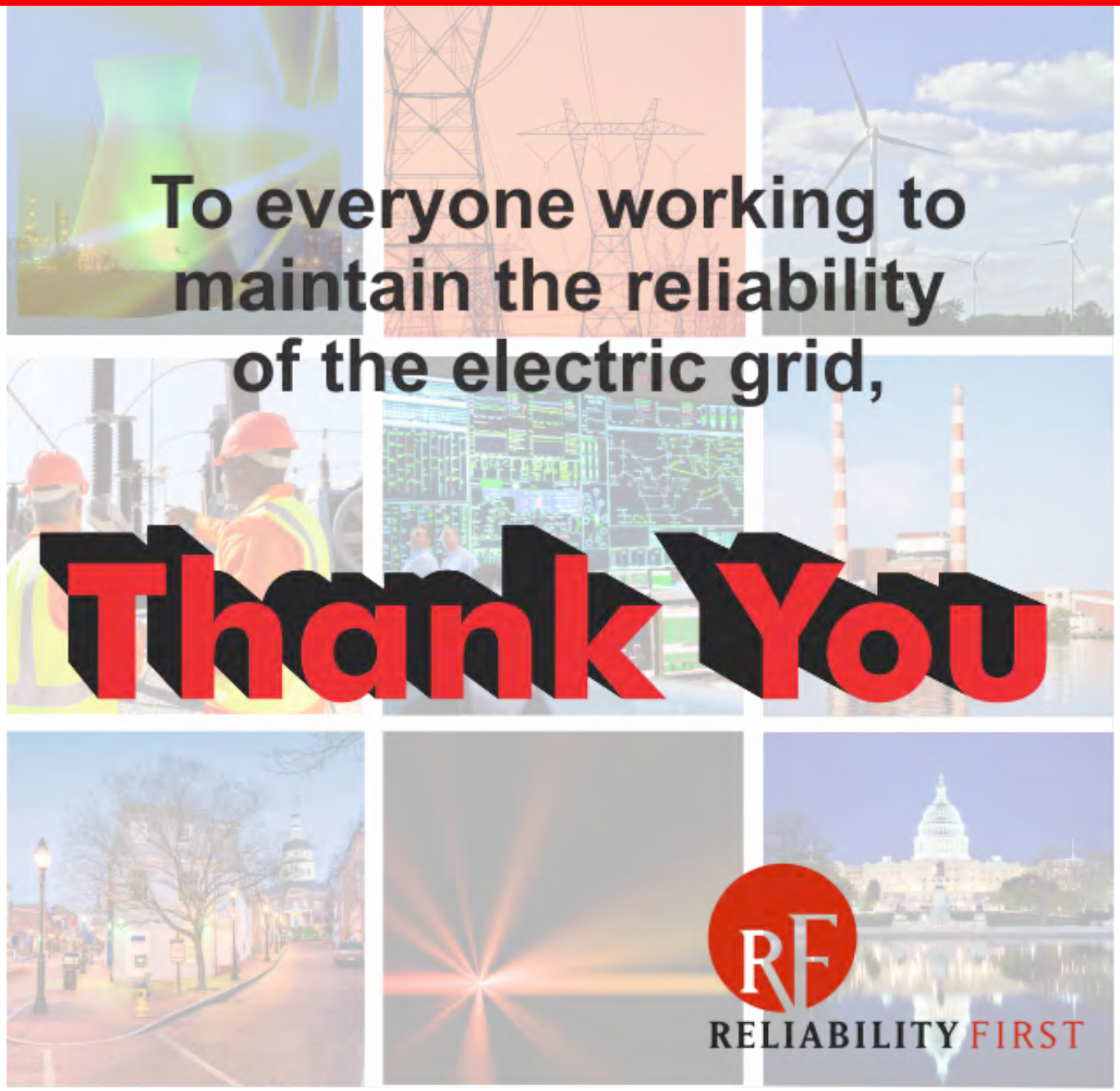
RF Publishes CIP Evidence Request Tool Tips and Reminders Sheet

While it may be hard to believe we are in the fourth year of using the CIP Evidence Request Tool (ERT), Version 4.0 was recently released. The ERT was developed by the ERO to provide a common format for Requests for Information, help the ERO be more consistent and transparent in its audit approach, and allow entities to submit evidence more efficiently by understanding what types are required for audit. It is used by all the Regional Entities and FERC auditors when they lead a CIP audit.

In addition to ensuring you are aware of the changes made in the Version 4.0 update, RF's new ERT Tips and Reminders Sheet contains helpful information for completing your ERT.

Updates to the new version include wording changes to the Level 1 and Level 2 tabs to clarify some of the requests. Additional Level 1 and Level 2 requests were added for CIP-003-8 - Cyber Security - Security Management Controls which will become subject to enforcement April 1, 2020.

Additional Level 1 and Level 2 requests were added for 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; and a procurement population tab was also added to allow for sampling of CIP-013-1.



During these uncertain times one thing is certain: there is an amazing group of dedicated people working tirelessly to ensure our electric grid is secure and reliable. Keeping the power on is fundamental to our most basic needs, and the RF team could not be more grateful to each and every one of you.

From the control center operations teams, to the linemen and crews in the field and everyone in between, RF is proud to work with such fantastic people!

Protection System Workshop for Technical Personnel
August 18-19, 2020

ReliabilityFirst is hosting its sixth annual protection system educational workshop for technical personnel on August 18-19, 2020 at the ESC Conference Center in Cleveland, OH. There is no fee to attend, and it is open to anyone who is interested.

This workshop will cover a diverse range of topics and discussions relative to Protection Systems tailored to the needs of technical personnel and will feature speakers from RF, industry subject matter experts and others. Topics slated for discussion include capacitor bank protection, protection simplicity, and IEC 61850 regarding communication in substation. This will be a highly interactive experience with an opportunity to share ideas, successes, questions and stories. There will also be vendor presentation and displays available during the event.

Intended Audience

- Substation Electricians/Supervisors
- Substation Field/Commissioning Engineers Relay Technicians
- Relay Engineers and others who work directly with this equipment
- Communications Engineers/Technicians
- Company Trainers on this subject
- Others interested in these topics

Register

Human Performance Workshop for Technical Personnel
August 19-20, 2020

ReliabilityFirst is hosting its third annual Human Performance workshop on August 19-20, 2020 at the ESC Conference Center in Cleveland, OH. There is no fee to attend this workshop, and it is open to anyone who is interested.

This workshop will focus on practical application of human performance techniques and concepts for front-line activities that attendees can use in transmission reliability-related work areas such as operations, asset management, design, protection, maintenance and others. Confirmed speakers include Dr. Jake Mazulewicz, Knowledge Vine, and Wes Harvard of Luminant Energy.

There will be an interactive session and industry speakers sharing ideas, successes and stories.

Intended Audience

- Substation and Transmission maintenance
- Protection and Controls
- Operations Control Rooms, including tools support personnel for EMS, SCADA, etc.
- Asset Design groups (substation and transmission)
- Asset Management groups
- Other leaders interested in these topics

Register

2020 Human Performance Improvement Overview
August 19, 2020

New this year, the Human Perf Improvement Overview is a pre-workshop educational session taught by Dr. Jake Mazulewicz. There is no fee to attend this session, and it is open to anyone who is interested. Space will be limited to 35 attendees.

Register

ReliabilityFirst Board of Directors and Committee Meetings will be held June 3-4, 2020

Calendar of Events

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

Date	RF Upcoming Events	Location
June 3	ReliabilityFirst Board of Director Committee Meetings	Cleveland, OH
June 4	ReliabilityFirst Board of Director Meeting	Cleveland, OH
May 18	Reliability and Compliance Open Forum Call	Conference Call
June 15	Reliability and Compliance Open Forum Call	Conference Call
July 20	Reliability and Compliance Open Forum Call	Conference Call
August 12	ReliabilityFirst Board of Director Committee Meetings	Chicago, IL
August 13	ReliabilityFirst Board of Director Meeting	Chicago, IL
August 17	Reliability and Compliance Open Forum Call	Conference Call
August 18-19	6th Annual Protection System Workshop for Technical Personnel	Cleveland, OH
August 19	HP Improvement Overview	Cleveland, OH
August 19-20	3rd Annual Human Performance Workshop	Cleveland, OH

Industry Events:

Date	Industry Upcoming Events
April 29	NERC - Industry Webinar: Risks and Mitigations for Losing EMS Functions Reference Document - Version 2
May 21	FERC - Open Meeting
June 18	FERC - Open Meeting
June 23-25	FERC - Technical Conference regarding Increasing Market and Planning Efficiency and Enhancing Resilience through Improved Software, Washington, DC
June 25	FERC - Technical Conference regarding reliability of the Bulk-Power System, Washington, DC)
September 1-2	NERC - GADS Wind Training
September 23-24	NERC - Monitoring and Situational Awareness Technical Conference, Golden, CO
September 29- October 1	NERC - Electric Power Human Performance Improvement Symposium, Denver, CO
October 20-23	NERC - GridSecCon (no location noted)

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