Issue 5
2019 September October

INSIDE THIS ISSUE



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

Follow us on:


# Note from the President

**Dear Stakeholders,**

I was pleased that many of you were able to experience a little Cleveland Fall this month at our Workshop. In this issue, you will see a recap of many of the reliability and security issues discussed. A focus of the Fall Workshop was Grid Transformation, and as various presenters, and particularly the industry panel, reiterated, it is an issue that involves collaboration and coordination. To that end, we work very closely with the RTOs in our Region and, you will see throughout this issue, they have recently spoken at our Board Meeting, collaborated on training with our staff, and graciously shared their knowledge with us as presenters and panelists at our workshop.

I was personally pleased to see many of you at the CIP focused day of our Workshop. We continue to see CIP violations increasing in our Region and across the ERO, so I continue to urge stakeholders to use the RF and ERO resources to assist their entities in strengthening their security posture. In the face of these complex risks, I'm encouraged by the ERO enterprise leadership and have seen great strides in the teamwork and support. I believe having all of us unified under the ERO enterprise strategic vision will allow us to collaboratively tackle the ongoing challenges that face our grid.

On the topic of industry partnerships, I recently brought Jim Robb and Mark Lauby of NERC to spend the day with the AEP team learning about their forestry, system operator training, system operations, and compliance programs. We were afforded the unique opportunity to fly over 765 kV line corridors, to experience what it is like to monitor vegetation maintenance from that perspective. We also toured AEP's newest 765 kV substation and got to see firsthand the physical security enhancements they included in the station's design. My sincere thanks to all those at AEP who made time for us to learn. It will help all of us make more informed decisions.

I also had the opportunity recently, along with Sara Patrick of MRO and Jason Blake of SERC, to spend the day with the MISO executive and compliance teams. During the visit, we learned more about MISO's re-envisioning of its compliance philosophy, met key members of the compliance organization, and were given the opportunity to interact with the entire compliance team in a panel, Q & A session. I always get a lot out of visits such as these and I am always happy to visit with our industry partners. If you would like me to stop by to see you, please just let me know.

Forward Together,

Tim

# From the Board

## August 22, 2019 RF Board of Directors Meeting Highlights:

### Keynote Speakers:

**Paul Thompson**, Chairman, CEO and President of Louisville Gas and Electric Company (LG&E) and Kentucky Utilities Company (KU).

Mr. Thompson emphasized that LG&E/KU customers, like all customers, want reliable, safe, secure and clean delivery of energy, and his company takes this shared responsibility very seriously. However, LG&E/KU, like many others, sees its greatest threats to this shared responsibility in the area of cybersecurity, an evolving resource mix, and an upward pressure on ensuring rates and costs are contained.


**Jim Robb**, President and CEO, NERC.

Mr. Robb presented the ERO Enterprise long-term strategy which centers on the primary reason for the ERO's existence; to assure a highly reliable and secure bulk power system for the benefit of society. To this end, Mr. Robb shared the ERO Enterprise's long term strategic focus areas, including the expansion of risk-based focus in all standards, compliance, and enforcement efforts. He also discussed how NERC is taking steps to mitigate new and emerging risks to reliability, and building a strong E-ISAC based security capability. Additionally, rounding out the strategic focus areas, Mr. Robb noted that the ERO Enterprise will look to strengthen engagement and collaboration across the reliability ecosystem, and capture effectiveness, efficiency and continuous improvement opportunities.


**Suzanne Keenan**, NERC Board of Trustees.

Ms. Keenan, one of the more recent NERC Board appointees, offered her observations to the Board as a relative "newcomer" to the industry, given that her last work with the industry was somewhere in the area of 20 years ago. She observed that so much has evolved in those 20 years and her observations so far have centered on several key areas. First, talent: can the industry continue to attract the type of talent needed in this new era to ensure critical mission success. Secondly, how do we – the ERO enterprise – continue to grow and align organizationally so as to drive one purpose and one goal. Lastly, Ms. Keenan noted that it will require great effort on behalf of the ERO enterprise, and the industry, to ensure that it can keep up with the rapid pace of change and ahead of evolving threats.

**Mike Bryson**, Senior Vice President, Operations, PJM.

Mr. Bryson gave a presentation to the Board on PJM's analysis of fuel security to assess deliverability as a result of changing resource mix and retirements well into the future. PJM worked with its stakeholders and several government agencies to develop key model assumptions as a way to conduct the analysis, and after analyzing more than 300 different scenarios, PJM concluded that in only several of the most extreme cases would it see any disruptions of service. Mr. Bryson noted that PJM continues to build upon its analysis to develop even more scenarios and plans to work with its stakeholders to address any issues that are revealed as a result of these studies.

# Get Control of Yourself

*By: Denise Hunter, Principal Technical Auditor*

***Please note when reading below, this was written following the Browns thrilling victory over the Ravens, but before the devastating loss to the 49ers. This goes to further emphasize the need that internal controls need to be sustainable and monitored so that we don't take a step backwards and bad habits don't re-emerge.***

***Its fall and the Browns are currently #1 in the AFC North!*** Now that I have your attention, you might wonder, what does that have to do with internal controls? Well, if you have ever heard me speak at one of the RF Compliance Workshops, you know that I explain an internal control as "any activity that you do to ensure that what you want to happen, happens, and what you don't want to happen, doesn't happen."

In my opinion, the Browns are working through the process of identifying their key controls. They have performed a few walk-throughs, found issues, and corrected them. Now, all they need to do is perform them consistently and monitor them to ensure they are still effective! But, as any true Browns fan knows, there is the nagging concern in the back of my mind that the Browns will discard their controls and return to previous activities, thus exemplifying the ERO Risk Element that I would like to address this month: ***The Inhibited Ability to Ride Through Events***. I'll leave the gridiron now and focus on the grid.

What exactly does this risk mean? The 2019 ERO Enterprise Compliance Monitoring and Enforcement Program Implementation Plan states, "Increased implementation of inverter-based resources has brought a focus on this issue. The ERO continues to raise awareness on inverter-based resource performance through NERC Alerts and industry outreach. Compliance monitoring should seek to understand how entities manage the risk of resource availability in this changing environment."

The industry is now aware that this risk is a growing concern. If you had the opportunity to attend the RF 2019 Fall Workshop, either in person or via WebEx, then you probably remember various presentations on Grid Transformation, including the panel discussion facilitated by Brian Thiry, Manager of Compliance Monitoring O&P. The panel was an opportunity for an open discussion regarding the reliability and resiliency risks the industry and our region faces, due to the changing landscape of the industry. Entity participants and the panel discussed some of the actions that they felt were needed in order to achieve reliability and resiliency in this environment. Ideas ranged from the need to consider retail effects on the grid upstream plus more collaboration, not only between utility organizations, but also between all stakeholders widening the circle to include cities, states, industry task forces, committees and forums in order to draw solutions from all areas.

The panel discussion also identified the steps that NERC has taken in order to address this risk by moving from a compliance based process to a risk based one. Some newer Standards raise the risk, but allow the industry to identify the extent of that risk as it applies to them, and mitigate it appropriately. With the rapidly changing grid, the fact that new Standards cannot always keep up with the changes, and the expectation of the public that we ensure we have done everything we can to ensure the security of the grid, the movement to a risk based process could not be timelier.



Continued on page 4

# Get Control of Yourself

*Continued from page 3*

The panel closed with an in-depth discussion on Distributed Energy Resources (DER). One of the issues that is becoming more prevalent is the popularity of DER and the fact that the Standards address BES risk, but have no jurisdiction over DER behind-the-meter. Again, the conversation shifted towards the need for the ERO, down to the utility level, to get more involved with their customers in order to obtain operating characteristics to facilitate the determination of the risk to the system.

So where am I going with this? Well, if you look at the Standards that we do have in place that address the risk of the inhibited ability to ride through events, coupled with the compelling conversations exhibited during the panel discussion at the workshop, you will notice a few themes bubble to the top: *the need for coordination, communication, and integration*.

My internal control focus for this issue will be on **Integration Control**.

What exactly is an Integration Control and why would we need it? An Integration Control is a process of establishing lists of inputs and outputs that affect the risk to grid reliability. It is the process of bringing together sub-systems or components of a subsystem, into one system. Identifying the components, applications, infrastructure, etc. into or alongside existing systems.

So what does that entail? In my opinion, it could consist of the following process steps[1]:

1) It starts with determining what you expect to gain. There is no such thing as a *standard* integration. Every company, department, etc. uses different processes, systems, tools to achieve different goals. Therefore, it is imperative that with each integration you determine your end goal (i.e. identify what you want to happen, happens).

2) Identify the multiple components and determine if integration needs to be performed in a certain order. A proper architecture design allows for a more efficient integration. (i.e. identify the process steps needed to achieve the outcome you want).

3) The next step is the most challenging: the performance of actual integration. Depending on the number and size of the various independent systems, information, or the data to be connected into one process, the outcome you are expecting may take some time. Especially while ensuring the regular data flow continues during this process.

4) The next step is critical. Once the system is ready, verify and test the integration. This is imperative in order to ensure that the product you receive meets expectations. That is why the implementation phase may take a while (i.e. what you expected to gain is met and this is ensured through the verification and validation process).

5) Then, as always, monitoring of the end product, with variations in the tests to ensure the process is being performed consistently and continues to produce the desired outcome.

A possible example of an integration process for DER could be an app similar to the Power Cost Monitor app. The Power Cost Monitor app was developed to help homeowners wirelessly monitor their energy consumption. A similar app could be designed to monitor roof top solar panel production, and then utility companies could integrate that information in order to better address that risk to the system.

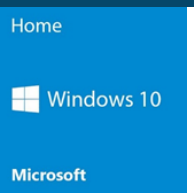
The ERO has recognized that we have challenges ahead with the rapidly changing landscape of our industry. However with diligence, and the design, implementation and monitoring of proper controls, we can ensure that we have provided reasonable assurance that the industry has in place the needed checks, to ensure the reliability and resiliency of the grid is attained.

With that, I will close with GO BROWNS! and we'll talk again soon.


[1] https://headchannel.co.uk/6-steps-of-system-integration-process-321

# Microsoft Windows 7-End of the Road

*By: Tony Freeman, Senior Risk and Mitigation Analyst*




January 14, 2020 is quickly approaching which will mark the end of the road for Windows 7. After a decade long lifecycle for this popular Operating System (OS), Microsoft will discontinue all support, extended support, and all updates for this once and still very popular OS. This all boils down to "use at your own risk" as security updates will no longer be provided potentially leaving your systems vulnerable to emerging cyber threats.

What does this mean for us? This should spark some thoughts, concerns, and questions into future Windows 10 upgrade. Though Microsoft is scheduled to release reminders and notifications through update KB4493132 it is important to start the upgrade early to avoid situations where support may be required after the January 14, 2020 cutoff. This should provide your organization sufficient time to properly test and implement the upgrade to Windows 10 or provide time to allow for the evaluation and implementation of a new platform in order to properly secure your protected environment(s).

Now, Microsoft is offering an "extended support" contract which will cost $25 per device the first year, $50 per device the second year, and $100 per device for the third year. Granted this can be fairly expensive considering the size of the environment and Microsoft is hoping that by 2023 that the number of users for Windows 7 is so small that they can stop offering support all together. With this, there are some additional options such as Windows 10 or platform replacement such as Linux.

You may find yourself pondering the move from Windows 7 to Windows 8 in order to save some money, but let's not forget that like its predecessor, Windows 8 will be end of life January 2023 and is currently operating like Windows 7 under the fairly expensive "extended support" period/ contract.

What should you expect with a Windows 10 upgrade? To start let's take a look at the requirements needed per system in order properly implement Windows 10.

- ***Processor of 1GHz process or faster***
- ***Memory of 1 GB RAM for 32-bit installations or 2GB of RAM for 64-bit installations***
- ***Hard Disk Space of 16GB for 32 –bit installation and 20GB for 64-bit installation***
- ***Graphics considerations consisting of Screen resolution of at least 800x600 and DirectX 9 graphics card with WDDM 1.0 driver***


Though the minimum specifications, Microsoft still recommends a system use a 2GHz dual core processor, 8GB RAM and 160GB hard drive. Since both of these Operating Systems are provided by Microsoft this means that disruptions from Windows 7 to Windows 10 should be minimal and most system and user files should go unaffected by the upgrade. However, it is always best to err on the side of caution and follow best practices and ensure you backup systems prior to a major upgrade such as this.

Other options include migrating to a new OS such as Linux Mint, which offers a User Interface similar to that of Windows 7. This OS also provides a variety of tools that are available upon installation. Other open source options are LibreOffice as an alternative to Microsoft Office, and WINE which allows most Windows applications to run on Linux. System administrators and users must also consider the compatibility of all systems, applications, and tools in their infrastructure when preparing for a major overhaul such as a Windows upgrade or migration.

Regardless of the path chosen, it is imperative that one starts to mitigate the impending risks surrounding the end of life of Windows 7 by properly planning to either upgrade or migrate existing Windows 7 devices. With this being said, remember to keep security best practices in mind prior to, during, and after this transition. This includes ensuring backups are taken, disaster recovery and back-out plans are current, testing has been completed, security controls implemented and verified, change controls have been approved, systems patches/ updated, and baselines updated in order to prevent any potential situation where a vulnerability may exist.

*If you have any additional questions, comments, or concerns regarding Risk Analysis, Mitigations, or Evidence please feel free to contact the ReliabilityFirst Risk Analysis and Mitigation (RAM) department here and ensure in the area field that you select "Risk Analysis & Mitigation."*

# 2019 Long Term Reliability Resource Assessment

RF performs an annual resource assessment based on the data PJM and MISO provide to RF. This article will share some highlights from that assessment. Based on the data received for the next 10-year period, PJM is expected to meet its reserve margin target through 2029.

The MISO reserve margin, which includes Existing-Certain and Tier 1[1] resources, satisfies its reserve margin target through 2024. The MISO reserve margin projected for 2025 is 647 MW below the reserve margin target. Continuing in 2026, the projected reserve margin is 773 MW below the target, and continues to decline to 3,075 MW below the target in 2029. Since these projected reserve deficits are six years into the future, RF staff believes that this range of reserves should be marginally acceptable. Six years lead time should be sufficient to manage resource adequacy. However, resource adequacy issues for these years will need to be closely monitored.

## PJM

**Capacity and Reserves**

PJM resources are projected to be 205,256 MW in 2020 and then increase to 220,488 MW by the end of 2029. The reserve margin calculations include planned generation retirements, planned generation additions and changes, and 50 percent of the Tier 21 projects from the generation interconnection queue. PJM is expected to meet its reserve margin target through 2029.

**Demand**

PJM RTO is projected to average a 0.42 percent load growth per year over the next ten years. The PJM RTO summer peak demand in 2020 is projected to be 150,870 MW and increase to 156,689 in 2029 for total internal demand (TID). The net internal demand (NID) is 141,743 MW in 2020 and increase to 147,256 in 2029 MW a 10-year increase of 5,819 MW and 5,513 MW, respectively. Annualized 10-year growth rates for individual PJM transmission zones range from -0.3 percent in Atlantic Electric Company to 0.9 percent in Dominion.

## MISO

**Capacity and Reserves**

MISO resources are projected to be 147,254 MW in 2020 and then increase to 197,079 MW by the end of 2029. This reserve margin calculation includes planned generation retirements, planned generation additions and changes, and Tier 2 and Tier 3 projects from the generation interconnection queue. MISO's anticipated reserve margin, which includes existing generation and Tier 1 resources, satisfies the target through 2024. The MISO anticipated reserve margin projected for 2025 is 647 MW below the reserve margin target. Continuing in 2026, the projected reserve margin is 773 MW below the target, and continues to decline to 3,075 MW below the target in 2029.

**Demand**

The 2019 forecasted MISO annual growth rate for 2020-2029 is approximately 0.22 percent. The MISO RTO summer peak demand is projected to be 124,809 MW in 2020 and 127,316 MW in 2029 for TID is 118,850 MW in 2020 and 121,324 MW in 2029 a 10-year increase of 2,507 MW and 2,474 MW, respectively.

## RF

**Resources**

The amount of generation capability for 2020 in RF is projected to be 222,059 MW. Overall, there is an increase in capacity through 2029 to 254,414 MW.

**Demand**

The estimated coincident NID peak of the entire RF regional footprint for the summer of 2020 is projected to be 165,173 MW. For the summer of 2029, NID is projected to be 168,580 MW. The compound annualized growth rate (CAGR) of the NID forecast is 0.23 percent from 2020 to 2029. The TID for the summer of 2020 is projected to be 175,369 MW. For the summer of 2029, TID is projected to be 179,009 MW. The compound annualized growth rate (CAGR) of the TID forecast is 0.23 percent from 2020 to 2029.

[1] Capacity categories listed in the LTRA are identified as either "Existing-Certain", "Tier 1", "Tier 2", or "Tier 3" resources. "Existing-Certain" and Tier 1 resources receive 100% capacity credit, while "Tier 2" and "Tier 3" resources receive varying capacity credit, due to the uncertainty of future project completion.



Continued on page 7

# 2019 Long Term Reliability Resource Assessment

*Continued from page 6*

**FIGURE 1**
**PJM RTO**
**Summer Reserve Margin Projections**
**2020 - 2029**

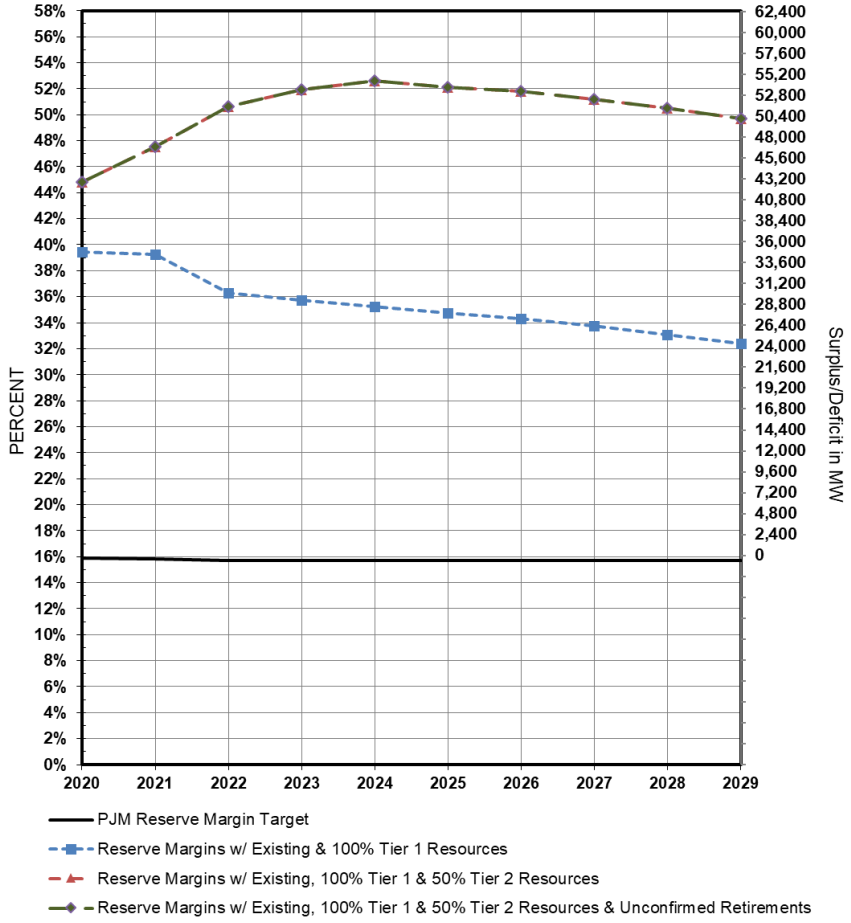
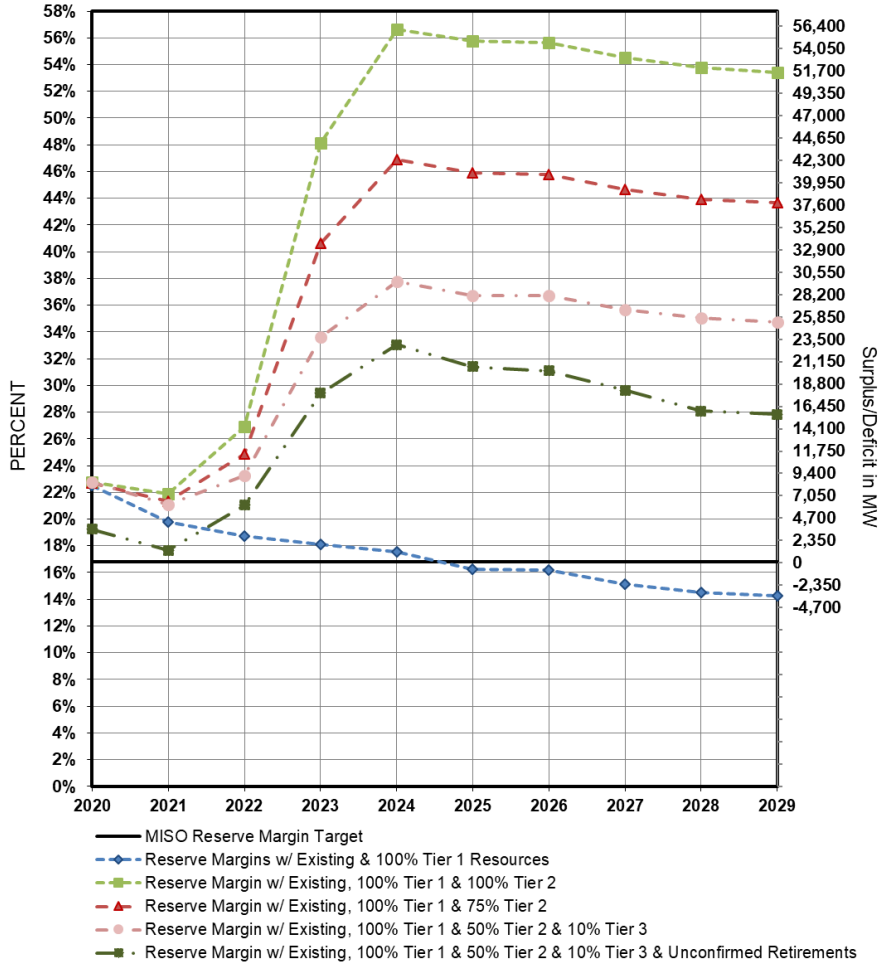



**FIGURE 2**
**MISO RTO**
**Summer Reserve Margin Projections**
**2020 - 2029**




*Figures 1 and 2* display graphs of the reserve margins for the PJM and MISO RTOs. The graphs include different scenarios including the unconfirmed retirements and Tier 2 capacity and, for MISO, Tier 3. The scenarios use percentages of the Tiers to gauge how much of the Generation Queue is needed to stay above the reserve margin requirement. The percentage included in these scenarios are on-top of the MISO confident factors. Generator retirements are evaluated by the RTOs for reliability impacts as each retirement is proposed. If the RTO determines that reliability impacts exist, the unit owner is asked to defer retirement until the reliability impacts are addressed. In this assessment, all confirmed generator retirements are assumed to occur after any reliability concerns are addressed. Unconfirmed Retirements are resources that are considered likely to retire by resource owners, but the formal notification has not been submitted to the respective RTO or to regulatory bodies. Also included in Unconfirmed Retirements are units for which such notice has been made, but a reliability impact assessment and potential designation as a reliability must run unit by PJM or MISO, is pending.



Continued on page 8

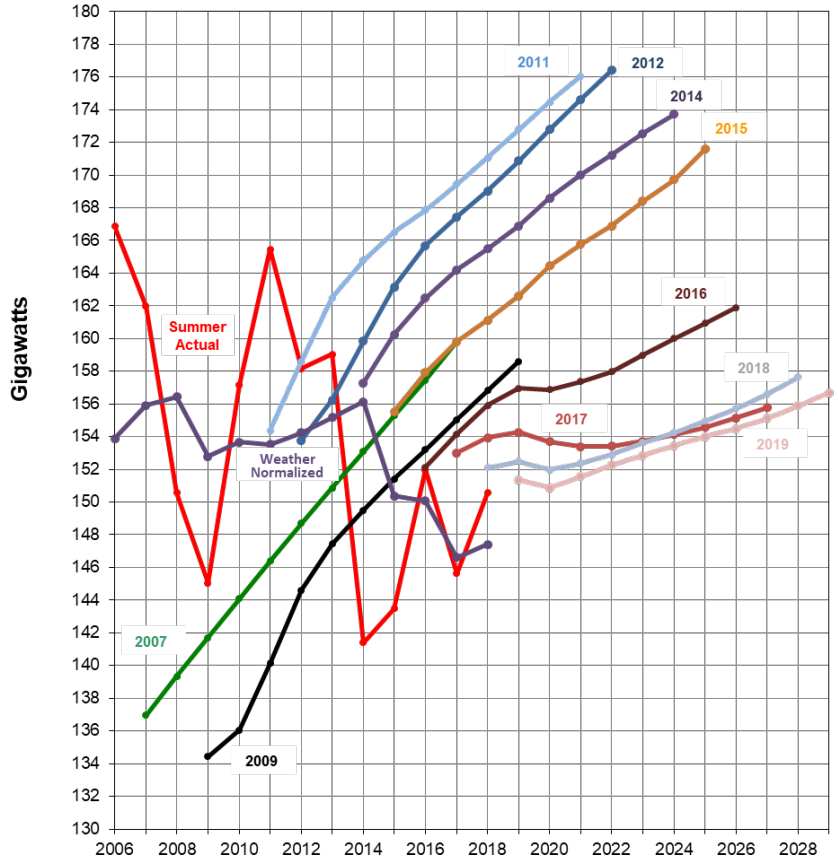
# 2019 Long Term Reliability Resource Assessment

*Continued from page 7*

*Figures 3 and 4* show comparisons of actual demand data to ten year forecasts of demand.

**Figure 3**
**PJM RTO Peak Demand Data**

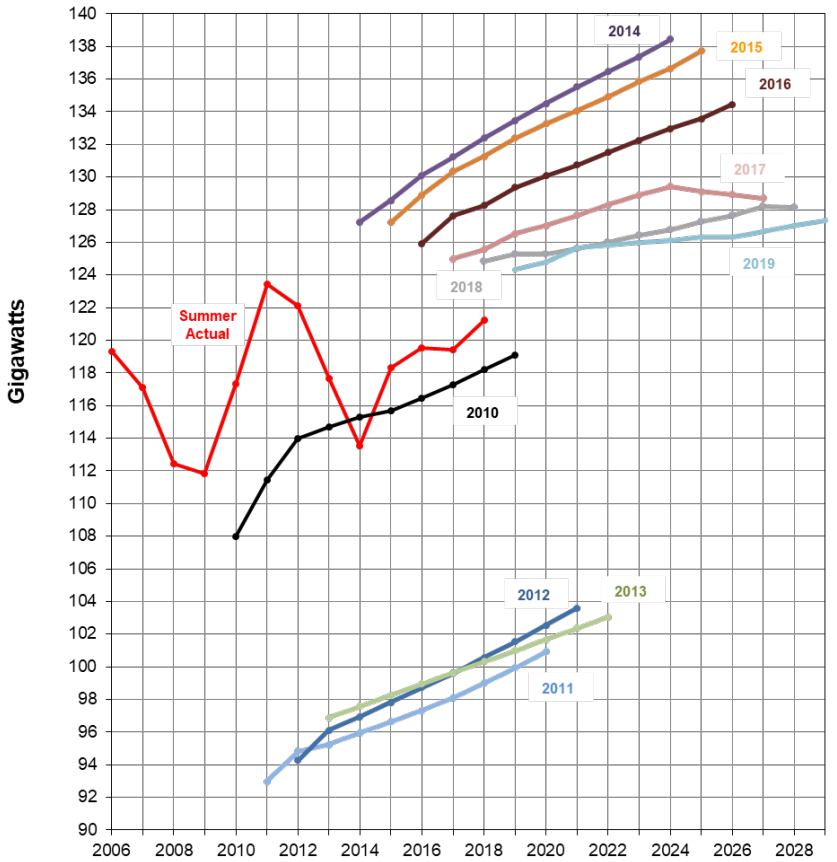
**Actual 2006 - 2018**
**Select 10 Year TID Forecasts Through 2029**




2011 Includes the expansion of the PJM RTO footprint with First Energy (ATSI) and Duke Energy Ohio and Kentucky
2013 Includes the expansion of the PJM RTO footprint with East Kentucky Power Cooperative
2019 Includes the expansion of the PJM RTO footprint with Ohio Valley Electric Cooperative

**Figure 4**
**MISO RTO Peak Demand Data**

**Actual 2006 - 2018**
**Select 10 Year TID Forecasts Through 2029**




2011 Includes the reduction of the MISO RTO footprint with First Energy (ATSI), Cleveland Public Power and Duke Energy Ohio and Kentucky moving to PJM RTO
2014 Includes the expansion of MISO RTO footprint with MISO South

# The Lighthouse

*By: Lew Folkerth, Principal Reliability Consultant*

## Low Impact Update and Final Check; Supply Chain Update

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.

**Low Impact Update**

There are three pending changes to the Reliability Standards that will have an effect on entities with low impact BES Cyber Systems.

***CIP-003-7***

CIP-003-7 will become effective on January 1, 2020.

The Implementation Plan for CIP-003-7 states that CIP-003-6 Attachment 1 Sections 2 and 3, the sections governing physical and electronic access controls, do not become enforceable. Instead, they are replaced by CIP-003-7 Attachment 1 Sections 2 and 3 which become enforceable on January 1, 2020. Additional changes in CIP-003-7 are discussed below.

***CIP-003-8***

CIP-003-8 will become effective on April 1, 2020, just three months after the effective date of CIP-003-7. The only change to the enforceable language of the Standard is the addition of a requirement to mitigate detected malicious code in third-party Transient Cyber Assets (TCAs).

***CIP-012-1***

As I write this, CIP-012-1 is pending regulatory approval. If approved, CIP-012-1 will be applicable to all Control Centers, including those BA and GOP Controls Centers that contain only low impact BES Cyber Systems. I plan to cover CIP-012-1 in depth in a future article.

Fort Gratiot Lighthouse, Port Huron, MI - Photo by Lew Folkerth

**Low Impact Final Check**

Since the effective dates of CIP-003-7 and CIP-003-8 are rapidly approaching, it's time for a final check of your compliance posture for low impact BES Cyber Systems before these revisions go live. Below I list the Standards and Requirements that are applicable to low impact BES Cyber Systems and provide a brief summary of each Requirement.

The accompanying summaries are written from the low impact perspective only. Unless otherwise noted, the language from an older version is unchanged in the newer versions. Upcoming dates are italicized. You must refer to the Standards for the exact wording of each Requirement.

This "Low Impact Final Check" is written from the perspective of an entity that has low impact BES Cyber Systems only.

If you also have high or medium impact BES Cyber Systems, many of your policies, processes, and procedures can be adapted to encompass your low impact BES Cyber Systems as well.



Continued on page 10

*Continued from page 9*

***CIP-002-5.1 R1 Part 1.3 (Effective Date July 1, 2016)***

You are required to identify each asset (such as a Control Center, substation, or generating facility) that contains at least one low impact BES Cyber System. While you are not explicitly required to identify each BES Cyber System at the low impact level, you may need to do so for other requirements. This is further explained in CIP-003-7 R2 Attachment 1 Sections 2 and 3, below.

Evidence for CIP-002-5.1 R1 Part 1.3 should include:

- Your determination of any assets that are not BES assets (assets with no component that meets the BES definition are out of scope for the CIP Standards);
- A description of how you determined that each asset contains (or does not contain) a BES Cyber System; and
- A description of how you determined that each BES Cyber System contained by the asset has a low impact rating (as opposed to a medium or high impact rating).

***CIP-002-5.1 R2 (Effective Date July 1, 2016)***

You are required to review the asset identifications from Part 1.3 every "CIP year" (15 calendar months). This review must be documented as audit evidence, and any changes to the asset identifications should be explained.

For example, if a new substation was commissioned, you should provide the commissioning date and any impact the new substation might have on the impact rating of neighboring substations. You also need evidence of your CIP Senior Manager's (or delegate's) approval for these identifications every CIP year.

**CIP-003-6 R1 Part 1.2 (Effective Date April 1, 2017)**

Cyber security policies that apply to the assets identified in CIP-002-5.1 R1 Part 1.3 must be documented. The policies must address four areas: cyber security awareness, physical and electronic access controls, and incident response.

Your evidence should include the documented policies, the review of these policies at least every CIP year, and your CIP Senior Manager's approval (no delegation permitted) at least once every CIP year.

***CIP-003-7 R1 Part 1.2 (Effective Date January 1, 2020)***

Cyber Security policies must be added to address Transient Cyber Assets (TCAs), Removable Media, and CIP Exceptional Circumstances at assets containing a low impact BES Cyber System.

***CIP-003-6 R2 Attachment 1 Section 1 (Effective Date April 1, 2017)***

Section 1 requires reinforcement of security awareness at least once every CIP year. You should keep evidence of the type and content of the reinforcement, the dates the reinforcement was provided, and that the reinforcement was provided to all groups, such as employees and contractors, who have access to assets containing low impact BES Cyber Systems.

***CIP-003-6 R2 Attachment 1 Sections 2 and 3 (No Effective Date)***

Sections 2 and 3 of version 6 will not become enforceable. They have been superseded by Sections 2 and 3 of version 7.

***CIP-003-7 R2 Attachment 1 Section 2 (Effective Date January 1, 2020)***

You are required to control physical access. You have two options to control access. You may choose to control physical access to the asset containing a low impact BES Cyber System or you may control physical access to the low impact BES Cyber Systems at the asset. I

f you choose to control physical access to the low impact BES Cyber Systems, you must be able to identify all BES Cyber Systems at the asset and show that physical access to each BES Cyber System is controlled.

You must also control physical access to Cyber Assets that control electronic access to low impact BES Cyber Systems. Your evidence will need to identify these systems and show that physical access to them is controlled.

These systems do not need to be located at the asset they are protecting (see Reference Model 3 in the Guidelines and Technical Basis). But wherever they are located you must control physical access to them.

Your evidence should include a description of the controls in place, and you should take credit for multiple layers of control if you use them. For example, you might list a gated and locked substation perimeter fence, a locked control house, and a locked equipment cage within the control house as layers of physical access control.

***CIP-003-7 R2 Attachment 1 Section 3 (Effective Date January 1, 2020)***

You are required to control routable electronic access to and from your low impact BES Cyber



Continued on page 11

*Continued from page 10*

Systems. The Guidelines and Technical Basis of CIP-003-7 contains ten Reference Models that explain possible methods of protection. Some reference models show protections for the entire asset containing the low impact BES Cyber Systems.

Others show protections at the BES Cyber System level. If you choose to protect just the BES Cyber Systems, you will need to be able to identify all BES Cyber Systems at the asset.

Your evidence should identify the types of access you permit and the business or operational need for the access. Remember that you must provide the justification for each type of permitted access, not just what the access is.

For example, just identifying that port 502 is permitted will be insufficient. You should state that the MODBUS/TCP protocol is permitted over port TCP/502 to and from switchyard equipment in order to monitor and control that equipment from the SCADA system.

Your evidence should include a discussion of how you meet the security objective of reducing the attack surface of your BES Cyber Systems through electronic access controls. Your discussion should also include why you think your controls will be effective in meeting the security objective.

If you permit dial-up access into a BES Cyber System, your evidence should show how you authenticate a dial-up user.

***CIP-003-6 R2 Attachment 1 Section 4 (Effective Date April 1, 2017; New Terms Effective January 1, 2021)***

Section 4 requires development and testing of Cyber Security Incident response plans for low impact BES Cyber Systems. Be aware that Section 4 relies on the NERC Glossary definitions of *Cyber Security Incident* and *Reportable Cyber Security Incident*, which will change when CIP-008-6 becomes effective on January 1, 2021.

Your evidence for Section 4 should include all incident response plans that are applicable to assets containing low impact BES Cyber Systems. You should be able show that each asset containing a low impact BES Cyber System has at least one applicable incident response plan.

Each incident response plan must include the components specified by Sections 4.1 through 4.6. Each incident response plan must be tested at least once every 36 months. When testing, be sure you can document that the incident response plan itself was actually tested.

One of the best ways to do this is to include an incident response checklist in your plan, and complete the checklist whenever the plan is tested. Keep the completed and dated checklists as evidence of testing of the plan. Note that you can use a response to an actual Reportable Cyber Security Incident as a test of the plan.

The last step in an incident response is usually a "lessons learned" review of the test or the actual incident. As no plan is ever perfect, you can usually find items to improve in your plan after each use of the plan. Track these items and be able to show that you have updated the plan within 180 days of the test or actual incident.

One way to do this is to keep a detailed revision history for the incident response plan, including the source of each change and the dates of the changes.

***CIP-003-7 R2 Attachment 1 Section 4 (Effective Date January 1, 2020)***

Version 7 of Section 4 updates the ES-ISAC reference to a reference to the E-ISAC.

***CIP-003-7 R2 Attachment 1 Section 5 (Effective Date January 1, 2020)***

Section 5 permits the use of, and requires controls for, TCAs and Removable Media at your assets containing low impact BES Cyber Systems. The existing NERC Glossary definitions of *Transient Cyber Asset* and *Removable Media* have been modified slightly to accommodate low impact considerations.

You must develop one or more plans to mitigate the risk of malicious code being introduced to a low impact BES Cyber System. Each plan should include provisions for TCAs managed by you, the Responsible Entity. The plan may call for managing these TCAs in either an ongoing or on-demand manner, or both. The plan also needs provisions for TCAs managed by a third party, such as a vendor or contractor. Finally, the plan must address detection and removal of malicious code on Removable Media.

Evidence for Section 5 should include each applicable plan, and each plan should show how you achieve the objective of mitigating the risk of introducing malicious code to a low impact BES Cyber System.

For TCAs managed in an ongoing manner, evidence should focus on the process of preventing malware from being introduced to the TCA. For TCAs managed in an on-demand manner, evidence should focus on the process used to ensure the TCA may be safely connected to a low impact BES



Continued on page 12

*Continued from page 11*

Cyber System prior to such use, including removal of any detected malicious code.

Evidence regarding use of Removable Media should include the controls used to ensure all Removable Media is cleared of any malicious code prior to connection to a BES Cyber System.

***CIP-003-8 R2 Attachment 1 Section 5 (Effective Date April 1, 2020)***

The only change to the enforceable language in CIP-003-8 is the addition of an explicit requirement to clean any malicious code from a third-party TCA before connecting the TCA to a BES Cyber System. Your plans should already require this, but be sure to review your plans to ensure they meet the new language.

**CIP-003-6 R3 (Effective Date July 1, 2016)**

You are required to document the identification of a CIP Senior Manager. Evidence of this designation must include the CIP Senior Manager's name, the date of the designation, and the date the designation was documented.

***CIP-003-6 R4 (Effective Date July 1, 2016)***

This Requirement permits the delegation of the CIP Senior Manager's authority as permitted by the Standards. For example, the CIP Senior Manager may delegate the authority to approve the list of assets containing low impact BES Cyber System, but may not delegate the approval of cyber security policies.

If delegations are used, evidence must include the name or title of the delegate, the specific actions delegated, the date of delegation, the approval of the CIP Senior Manager (usually a signature), and the date of the documentation of the delegation.

**Supply Chain Update**

The NERC Critical Infrastructure Protection Committee (CIPC) has issued five Security Guidelines and associated training materials related to supply chain cyber security. The Guidelines address five topics:

1. Risk Considerations for Open Source Software
2. Provenance
3. Cyber Security Risk Management Lifecycle
4. Secure Equipment Delivery
5. Vendor Risk Management Lifecycle

Each is a short (4-5 pages) paper accompanied by a training presentation. The papers and presentations are available on the NERC web site here (Security Guidelines - CIP Security.)

Note that these Guidelines are not directly compliance related. They are not Implementation Guidance, and they are not enforceable. Rather, they are a discussion of good security practices related to their specific topic. I recommend reading them, as they provide insight into various areas of supply chain cyber security that you may not have previously considered.

**Requests for Assistance**

If you are an entity registered within RF 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 rfirst.org web site here.

In addition, if you would like RF Entity Development staff to review your supply chain cyber security risk management plan and provide you with feedback, you can request this through the Assist Visit link above. Be aware that RF will not make compliance determinations in advance of an audit, but can only raise concerns and indicate areas for improvement.

## 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

## NERC 7th Annual Monitoring & Situational Awareness Technical Conference

RF's Events Analysis and Situational Awareness department attended the 7th Annual Situational Awareness and Monitoring Conference in Little Rock, Arkansas on September 24 and 25. At the conference, there were many different topics covered such as virtual Control Room tours, Analysis of EMS Outages, Situational Awareness Tools as well as vendor panels and Lessons Learned reviews.

Dwayne Fewless, from RF moderated an RTA (Real Time Assessment) panel that included several entities from across the ERO. During this panel, questions were asked of how these entities would respond when their primary tools failed in an effort to maintain the ability to continue to run RTAs. There was good interaction with the audience during this time as several questions were asked and answered.

Dwayne also presented on a NERC Lessons Learned that RF assisted in crafting. The Lessons Learned covered the importance of Alarming in the Control Room when it comes to tools such as State Estimator and RTCA (Real Time Contingency Analysis). This presentation covered 5 different scenarios that were received through the Events Analysis process.

## FERC Chairman Neil Chatterjee Publishes Editorial on Power Grid

On October 6, 2019, FERC Chairman Neil Chatterjee published an editorial entitled "The Power Grid is Evolving. Cybersecurity Must Too." The editorial argues that as foreign adversaries increasingly target America's critical infrastructure systems, FERC must continually evaluate its mandatory cybersecurity standards to allow utilities to harness the benefits of new technologies and to mitigate the associated risks. Chairman Chatterjee argues that any new cybersecurity standards must clearly address new technologies while still remaining flexible as technology is constantly changing. His full editorial can be read here

## FERC Staff Report Highlights Lessons Learned from CIP Reliability Audits

FERC oversaw audits conducted by NERC and regional entities of CIP Reliability Standards compliance. Most audits found no compliance violations, but some of the practices observed could lead to future violations. As a result, FERC published this Lessons Learned report available here.

The 7 Lessons Learned are:

**(1) Consider all generation assets, regardless of ownership, when categorizing BES Cyber Systems associated with transmission facilities.**

**(2) Ensure that all employees and third-party contractors complete the required training and that the training records are properly maintained.**

**(3) Verify employees' recurring authorizations for using removable media.**

**(4) Review all firewalls to ensure there are no obsolete or overly permissive firewall access control rules in use.**

**(5) Limit access to employee's PIN numbers used for accessing PSPs using a least-privilege approach.**

**(6) Ensure that all ephemeral port ranges are within the Internet Assigned Numbers Authority (IANA) recommended ranges.**

**(7) Clearly mark Transient Cyber Assets and Removable Media.**

# Standards Update

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

## General NERC Standards News

**Compliance Guidance Posted**

NERC posted the following guidance documents on its Compliance Guidance page:

- TOP-001-4 and IRO-002-5 Data Exchange Infrastructure and Testing Requirements (OC).

**Lessons Learned Posted**

NERC posted the following lessons learned on its Lessons Learned page:

- Loss of Monitoring or Control Capability due to Power Supply Failure
- RAS Unexpected Operation
- Inadvertent CVT Fuse Removal on a Live Circuit
- Breaker Failure due to Multiple Reclose Attempts
- Risks Posed by Firewall Firmware Vulnerabilities

**Reliability Guidelines Posted**

NERC posted the following guidelines on its Reliability Guidelines page:

- Reliability Guideline: Parameterization of the DER_A Model
- Reliability Guideline: Improvements to Interconnection Requirements for BPS-Connected Inverter-Based Resources

**Other Resources Posted**

NERC has posted the following additional resources:

- The slide presentation and streaming webinar for the August 2, 2019, Project 2019-01 – Modifications to TPL-007-3 webinar.
- The slide presentation and streaming webinar for the August 12, 2019 Electromagnetic Transient Modeling and Simulations in AEMO webinar.
- The slide presentation and streaming webinar for the September 5, 2019 Winter Preparation for Severe Cold Weather webinar.
- The slide presentation and streaming webinar from the September 12, 2019 Project 2016-02 – Modifications to the CIP Standards | CIP-005 and Associated Definitions.
- The slide presentation and streaming webinar from the September 13, 2019 Electromagnetic Pulse (EMP) Task Force webinar.
- The slide presentation and streaming webinar for the CIP-008-6 Requirement Training webinar.
- The slide presentation and streaming webinar from the September 23, 2019 Supply Chain Risk Assessment Data Request webinar.
- Supply Chain Security Guidelines and Training Presentations.

## Notable FERC Issuances

FERC issued no relevant orders in August and September.

## Notable NERC Filings

In August, NERC filed the following with FERC:

- Comments in Response to Notice of Proposed Rulemaking Regarding Proposed Reliability Standard TPL-001-5

NERC's filings can be found here.

# Standards Update

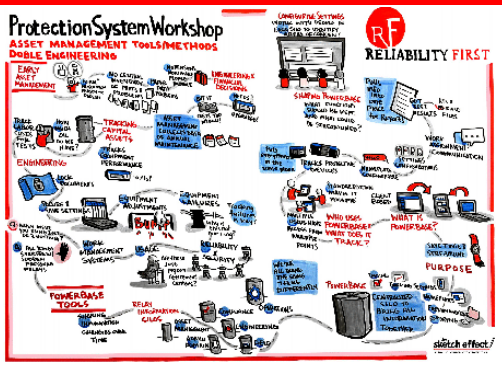
## New Standards Projects

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:

| | | |
|---|---|---|
| **2019-01 – Modifications to TPL-007-3** | **Initial Ballot and Non-binding Poll** | **08/30/19 – 09/09/19** |
| **2019-01 – Modifications to TPL-007-3** | **Join Ballot Pools** | **07/26/19 – 08/26/19** |
| **2019-01 – Modifications to TPL-007-3** | **Comment Period** | **07/26/19 – 09/09/19** |

| **Recent and Upcoming Standards Enforcement Dates** | |
|---|---|
| **January 1, 2020** | CIP-003-7 – Cyber Security – Security Management Controls; IRO-002- 6 – Reliability Coordination – Monitoring and Analysis; PRC-026-1 – Relay Performance During Stable Power Swings (Requirements 2-4); TPL-007-3 – Transmission System Planned Performance for Geomagnetic Disturbance Events (Requirements 5, 5.1, 5.2, 9, 9.1, and 9.2) |
| **April 1, 2020** | CIP-003-8 – Cyber Security – Security Management Controls |
| **July 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 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** | CIP-008-6 – Cyber Security – Incident Reporting and Response Planning; PRC-012-2 – Remedial Action Schemes |
| **July 1, 2021** | TPL-007-3 – Transmission System Planned Performance for Geomagnetic Disturbance Events (Requirements 11 and 12) |
| **January 1, 2022** | TPL-007-1- 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.




## Fifth Annual Protection System Workshop & Second Human Performance Workshop

RF hosted the fifth annual Protection System Workshop for Technical Personnel on August 13 and 14 at our Independence office and had more than 75 people in attendance, including speakers and vendors. The focus theme for this year was "Asset Management Tools/Methods, the future of Managing Protection System Settings and Data". 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!

Speakers from American Electric Power, FirstEnergy, and Duquesne Light discussed how their company handled the management of assets, protection system settings, and data. Vendor representatives from Omicron, Schweitzer Engineering Laboratories, and Doble Engineering presented their solutions for relay testing, utilizing substation data for monitoring and compliance, and data/asset management.

The workshop also included a breakout session where attendees formed into small groups to discuss various issues and their current practices or proposed solutions. This provided the opportunity for attendees to meet colleagues from other companies and talk about common issues and solutions.

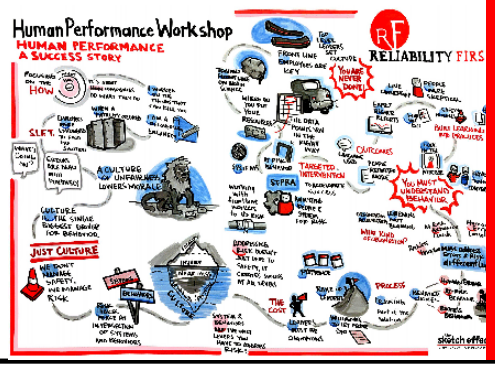
Immediately following the Protection System workshop, the second annual Human Performance Workshop kicked off with over 80 people in attendance. The Human Performance Workshop centered on a theme of creating and maintaining a culture that promotes Human Performance. This workshop focused on practical application of human performance techniques and concepts for front-line activities that attendees can retain and use in transmission reliability related work areas such as operations, asset management, design, protection, maintenance, and others.

Speakers from Consumers Energy, MISO, DTE Energy, and FirstEnergy shared their experiences with various human performance efforts they are undertaking. HP professionals Monika Bay and Jake Mazulewicz shared success stories they have been involved in and techniques they have developed.

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. 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.

These workshops are organized and coordinated by the Reliability Assessment and Performance Analysis (RAPA) department and provide an opportunity for Registered Entity personnel to interact with their counterparts, learn new techniques and procedures, and share experiences.

If you have questions, need more information, have topic suggestions or would like to present at future workshops, please contact Thomas Teafatiller, John Idzior, or Jeff Mitchell.




## Save the Date 2020

**Protection System Workshop**

**August 18-19**

**Human Performance Workshop**

**August 19-20**

**Cleveland, OH**

## RF Board Member Larry Irving Inducted Into the Internet Hall of Fame, the First African American to Receive the Honor

On September 27, 2019, the Internet Society inducted RF Board Member Larry Irving into the prestigious Internet Hall of Fame, which aims to "publicly recognize a distinguished and select group of visionaries, leaders, and luminaries who have made significant contributions to the development and advancement of the global Internet."

Mr. Irving is credited with coining the term "digital divide", which highlights the disparity of internet and technology access between different populations. In Mr. Irving's work, he has helped narrow the divide by bringing increased internet access to unserved and underserved populations. The digital divide has been, and continues to be, referenced by virtually every governmental, corporate, philanthropic, and non-profit organization across the planet that works to increase access to the internet and improve user competence in navigating the web. Mr. Irving is the first African American to be among the elite ranks of notable individuals inducted into the Internet Hall of Fame since its founding in 2012.

Mr. Irving produced the initial study on the digital divide while he served in the Clinton Administration as an adviser on telecommunications and information technology issues. He was one of the principal architects of the administration's telecommunications and Internet policies.

INTERNET
HALL of FAME

**RF Board of Directors**

**and Committee**

**Meetings will be held**

**in Washington, DC**

**November 20-21, 2019**

**click here for details**

# RF 2019 Fall Workshop Recap

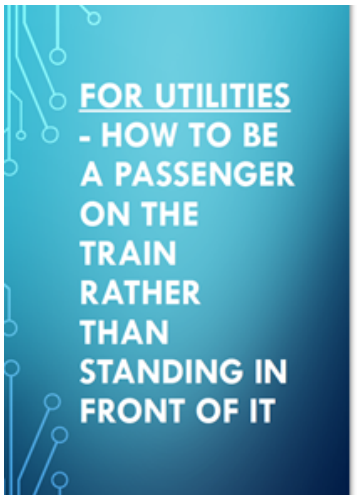
We would like to thank everyone who participated in our Fall Workshop, we had over 170 people join us in Cleveland and over 70 via Webex.

Day one, our Director of Compliance Monitoring, Jim Uhrin, welcomed everyone to our workshop. Thomas Coleman, Director, Power Risk Issue and Strategic Management at NERC delivered the keynote address.

He asked the audience, "How do we prepare ourselves for things that are unexpected?" and emphasized the point that volatility exists, and there are currently vast industry changes happening in the policy making and regulatory environment, so how do we recognize the volatility and manage it. He also pointed to a few relevant NERC resources.

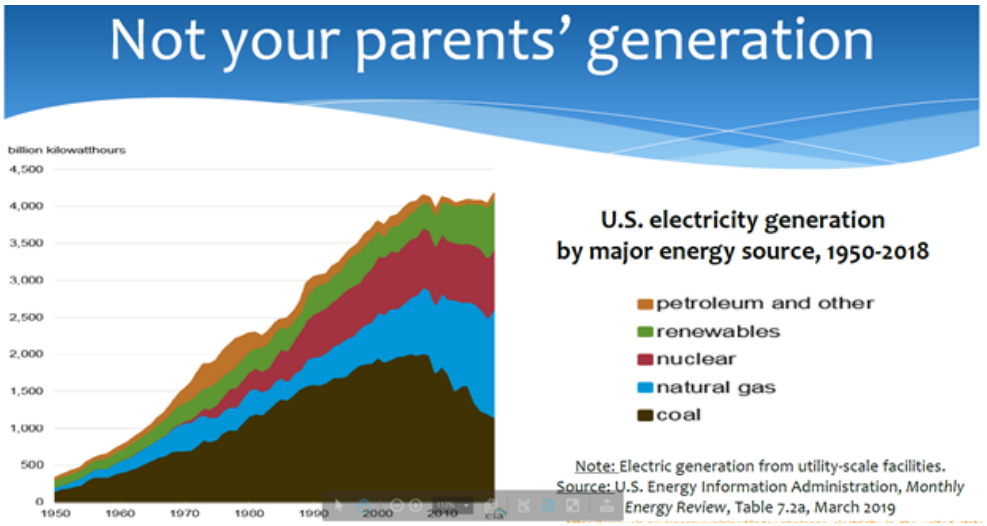
- 2019 Long-Term Reliability Assessment
- NERC ERSWG Page
- NERC 2019 State of Reliability
- NERC RISC Page

The focus of the morning was Grid Transformation. Roy Palk kicked off the morning with a discussion on Distributed Energy Resources. He shared that our industry was created in turmoil and always survived, so disruption doesn't mean destruction.





Next was Regulatory Changes and Impact to Compliance Matters, where Kristen Connolly McCullough followed with a walk through of recent environmental, regulatory and technology changes affected our industry. She addressed that the intersection of these changes often pose challenges for compliance managers struggling to maintain reliability, resiliency and smooth functioning of the bulk electric system. She ended the presentation with examples of such challenges and unintended consequences, including inverter failures. Her slides contain additional knowledge, and we'd encourage you to revisit the information she tailored for our audience.




PJM contributed two presentations on this topic. Daniel Bennett, Senior Engineer, Operations Planning presented on Fuel Security Related to the Changing Resource Mix. Natalie Tacka, Engineer, Applied Innovation, discussed the impacts and challenges of the changing resource mix on operational procedures in PJM. She highlighted recent efforts to enhance processes and tools that address gas pipeline contingency procedures, enhanced reporting for resource limitations, and visibility of DER in operational procedures.

MISO continued the discussion after lunch with a presentation, MISO Planning Relating to the Changing Resource Mix and The "MISO Forward" Effort Related to the Changing Resource Mix .



Continued on page 19

# Watt's Up at RF

*Continued from page 18*

MISO Forward focuses on the '3Ds' driving change on the electric grid:

- De-marginalization: incremental energy costs are approaching zero due to nonexistent or very low fuel costs
- Decentralization: shift away from large, central-station power plants to smaller, local generators
- Digitalization: revolution in information and communication technologies

The MISO region is expected to have adequate resources to meet its Planning Reserve Requirements for 2020. However, continued action will be needed to ensure sufficient resources are available going forward.

The MISO region continues to see a changing resource mix highlighting the importance of necessary reliability attributes for an evolving grid where "every hour matters".

MISO and its stakeholders continue to work through its Resource Availability and Need (RAN) initiative to address both near- and long-term reliability of the evolving grid.

To address the opportunities and challenges from these trends, MISO Forward identifies three core needs:

- Availability: ability of transmission and energy resources to meet requirements, 24/7/365
- Flexibility: ability to anticipate and adapt to changes in resources and demand
- Visibility: ability to see and coordinate resources and demand in operating and planning horizons

MISO utilized an insights-driven framework of "Explore, Decide, Do" to develop action plans to address each core need. Details for each need are documented in the MISO Forward Report and have been included in discussions of MISO's Integrated Roadmap, a stakeholder forum for MISO's annual issue prioritization process.

The morning speakers wrapped up our focus by participating on a Grid Transformation Panel discussion, which allowed the audience to ask questions around this complex topic and hear multiple perspectives.

Brian Thiry, Manager of Operations & Planning Compliance Monitoring, moderated the panel, keeping the focus on reliability and resiliency, while touching on a range of issues including the need for collaboration (between different regulatory groups, stakeholders, and even with the customers themselves), plus the challenges with forecasting what's behind the meter and outside FERC jurisdiction.

We were thrilled to have this diverse set of presenters join us and hope this helped to further holistic views and encourage community solutions to the grid transformation challenges.

That afternoon, RF and NERC provided updates, including the Electromagnetic Pulse EMP Task Force Update, an overview of the Compliance Oversight Plan Process Enhancements, and the status of the CORES and ALIGN projects.

Day Three resumed with a cybersecurity focus, and Matt Thomas, Manager, Compliance Monitoring, invited everyone back and introduced the keynote speaker, David Kennedy, from TrustedSec and Binary Defense. He provided a lively discussion of what is happening in the industry and the tactics, techniques and procedures of attackers.

The tactics of attackers are shifting, and it is important for the industry to understand that we can't protect everything out there, so the focus has to be on minimizing damage to your organization. He emphasized the importance of a quick response, and being aware of email structure and formatting, malware, and the general sophistication of attackers. He closed with three priorities: visibility, vulnerability management and the fact that while sophisticated attackers aren't slowing down, the industry as a whole is also getting more sophisticated.

RF's Senior Analyst, Tony Freeman led a discussion about Cyber Assets baselines, where he challenged the audience to think about their systems and talk through challenges and best practices.

Eric B. Smith, FBI Special Agent in Charge, Cleveland joined us to provide a Critical Infrastructure Security Update. NERC joined us to provide updates on the BCSI Practice Guide. RF provided an information session on Insider Threats Programs including a review of trends and the role of human factors and a quick update on GRIDEx V.

RF held a panel discussion on the topics of change and patch management. Panelists included representatives from MISO, FirstEnergy, and NRG. With respect to change management, good discussion was held around the different tools and controls that are available to help improve the efficiency and effectiveness of these processes and strategies for implementing these processes consistently across an organization.

On the topic of patch management, the audience and panelists engaged in constructive dialogue regarding challenges they face with managing their relationships with external parties, who are essential to the patch assessment and implementation process.

A focus of the afternoon was on CIP lessons learned. We had several presenters approach



Continued on page 20

# Watt's Up at RF

*Continued from pagee 19*

CIP-004 Lessons Learned, by going through a journey NIPSCO embarked on in order to improve their CIP-004 Access Management Program. It included a lookback to when NIPSCO was tracking many activities through numerous laborious manual processes. They walked through their decisions to improve the process and how to accomplish a more robust program and the implementation of the Alert Enterprise tool. They also went into their plan for future enhancements.

Also on the topic of CIP Lessons Learned, Scott Pelfrey, Principal Technical Auditor at RF went over lessons our auditors have identified as issues or areas of concern. He reviewed Electronic Security Perimeters (ESP) and access permissions under CIP-005 Requirement 1, and dove into Requirement 2 relating to Interactive Remote Access (IRA) and how NP-view is used to determine potential issues with IRA into the ESP. Finally he shared tips on what auditors are looking for and pitfalls they have seen over the past few years.

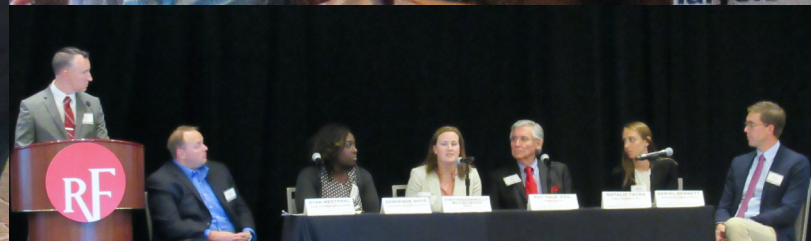
The day wrapped up with NP View Best Practices, presented by Don Miller, Account Manager and Robin Berther, Co-Founder of Network Perception. They discussed how to leverage technology such as NP-view to quickly identify firewall configuration issues and automate the CIP-005 ruleset review process. They also offered guidance to assist with network map visualization, ruleset review, and risk alerts, network access verification, and evidence collection and reports.

**Internal Controls Update**

Both days included an announcement sharing RF's excitement about the upcoming Internal Controls Workshop on February 12. In the meantime, check out the Internal Controls Knowledge Center page here for more information and our flashcards which have 16 internal controls that can help your performance.

We look forward to seeing you in February so we can work on this together!





## Save the Date

## Internal Controls Workshop

**February 12, 2020**

## AEP Flyover

Jim Robb, President and CEO, and Mark Lauby, Senior Vice President and Chief Engineer of NERC; and Tim Gallagher, President and CEO of RF participated in a flyover with AEP.

They spent the day learning about their forestry, system operator training, system operations, and compliance programs. They also flew over 765 kV line corridors, to experience what it is like to monitor vegetation maintenance from that perspective.

## PJM Training

RF was happy to host PJM, who provided training to RF, NERC and SERC personnel on September 30th, 2019. PJM covered a wide array of topics, from an overview of their system operations and planning to their energy markets.

Additionally, emerging technologies were reviewed to understand the tools PJM is developing to handle the changing electric utility landscape. Lastly, PJM provided an in-depth look into their control room, positions and tools used in the oversight of their footprint. Over 40 ERO staff were in attendance in person and via WebEx.

# Calendar of Events

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

| Date | RF Upcoming Events | Location |
|---|---|---|
| November 20 | RF Board of Directors Meeting | Washington, DC |
| November 21 | RF Board of Directors Meeting | Washington, DC |

## Industry Events:

| Date | Industry Upcoming Events |
|---|---|
| 10/17 | FERC Open Meeting |
| 10/22-10/24 | NERC TADS Conventional Training, Atlanta, GA |
| 11/5 | FERC Workshop regarding Grid-Enhancing Technologies (Washington, DC) |
| 11/14 | NERC Industry Webinar - Improvements to Compliance &Enforcement |
| 11/21 | FERC Open Meeting |
| 12/9 | NERC Industry Webinar - Improvements to Compliance &Enforcement |
| 12/10-12/11 | FERC Environmental Review and Compliance for Natural Gas Facilities Seminar (Seattle, Washington) |
| 12/19 | FERC Open Meeting |

### Illinois

Illinois is the fifth-largest energy-consuming state in the nation, and its industrial sector, which includes petroleum refining and coal mining, uses the most energy of any end-use sector in the state.

Illinois ranks fourth in the nation in crude oil refining capacity and leads the Midwest with a refining capacity of nearly 1 million barrels per calendar day.

The estimated coal reserves in Illinois are the second-largest after Montana, and the state's coal mines account for 6% of U.S. coal production.

Illinois has the third-largest ethanol production capacity (1.9 billion gallons) and the fourth-largest biodiesel fuel production capacity (184 million gallons).

Illinois ranked first in the nation in 2018 in net electricity generation from nuclear power, and the state's six nuclear plants accounted for 12% of U.S. nuclear power generation.

# 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