Issue 3
2019 May-June

INSIDE THIS ISSUE

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

Follow us on:

RELIABILITY FIRST

Note from the President

Dear Stakeholders,

I hope you are all enjoying the longer summer days. We know this poses operational challenges due to thunderstorms, tree growth, and peak demands and I appreciate your continued diligence to keep our lights and our air conditioners on.

This issue is longer, which I believe is a testament to all the hard work occurring in our Region and across the ERO. I am pleased with the results of the Summer Reliability Assessments highlighted in this issue. I commend NERC's most recent State of Reliability report to your reading. It is an excellent and informative report and it indicates that by all measures, 2018 was a highly reliable year for the North American bulk power system.

Internal Controls and Insider Threats are both areas of emphasis for our Region. There is a lot of information inside this issue that I hope you find useful as you evaluate and improve your supply chains, contractor use, and ongoing personnel management and employee access practices.

We believe outreach is a critical tool for achieving our collective mission and helping you pursue excellence. It is gratifying to see so many of you attend at our Spring Workshop, and the various subcommittee meetings, trainings, and technical workshops we've hosted. As you can see from these recaps, it's been busy, and as you will see from the Save the Dates there are several opportunities to collaborate in the coming months. Our Fall Workshop in Cleveland will provide a unique opportunity to consider the rapidly changing resource mix in our Region, and we hope you will join us as we delve into this with us as we consider the related risks and compliance implications.

Finally, I'll express my enthusiasm at welcoming Mr. Mattiuz to our Board. I continue to be impressed with the talent I'm surrounded by, and as you can see from our recent guests our Board also continually seizes opportunities to engage and learn with top talent. This collaboration truly makes us better at executing our critical mission and performing the role each of us plays in ensuring a highly reliable and secure bulk power system.

Forward Together,

Tim

Forward Together ReliabilityFirst

From the Board

RF held its Second Quarter Board of Directors meetings at its offices in Cleveland, OH from May 22-23, 2018. Three special guests provided keynote remarks:

Jennifer Flandermeyer

Jennifer Flandermeyer, Director of Federal Policy at Kansas City Power & Light Co. (KCPL), discussed the SPP RE dissolution process and KCPL's experience during that process as an entity that transferred from SPP RE to MRO. She also discussed the work of the NERC Compliance and Certification Committee, which she chairs. She noted that the Committee collaborates with NERC and the Regions to support regulatory success.

Mark Lauby

Mark Lauby, Senior Vice President and Chief Reliability Officer at NERC, discussed the value of innovation at the Regions, and praised RF's work in this area. He discussed efforts at NERC to further enhance guidance and knowledge sharing across the ERO Enterprise. He also highlighted key risks facing the electric grid, including cyber and physical security, critical interdependencies and complexities, the changing resource mix, situational awareness, and resource adequacy.

David Godfrey

David Godfrey, Vice President of Reliability and Security Oversight at WECC, discussed the benefits of the Regional model and the Regions leveraging ideas and sharing knowledge. He noted that WECC learned about RF's assist visit program, and now has a similar program for its entities.

RF Board of Directors and Committee Meetings will be held in Louisville, KY August 21-22, 2019

From the Board

RF is excited to welcome Bob Mattiuz as one of the newest members of the Board of Directors. He joins an impressive group, and we are grateful to have his expertise and look forward to his contributions. We have asked our new Director to share some of his experience with us and thoughts for the upcoming term.

Could you please tell us a little about your educational background and professional experience.

I received a Bachelor of Science degree in Electrical Engineering from Penn State University in 1984. Upon graduation, I started with West Penn Power Company, now a subsidiary of FirstEnergy. Later that year, I was ecstatic to be transferred to State College, PA, the home of Penn State! I subsequently earned a Master of Science degree in Industrial Administration from Carnegie Mellon University and my professional engineer's license in Pennsylvania.

Over my 35-year career at FirstEnergy, I've held various management positions in transmission & distribution engineering, planning and operations, as well as federal & state regulatory compliance, which included FERC and NERC oversight responsibilities. A major challenge in my career involved relocating my family from western Pennsylvania to northeast Ohio area in 2011. We love the area, but as a Penn State graduate, it's been difficult dealing with the Ohio State fans😊.

In May 2018, I was named Vice President, Compliance and Regulated Services and Chief FERC compliance officer for FirstEnergy. In addition to having oversight of FERC and NERC regulations, I am responsible for wholesale generation interconnections and agreements, energy market settlements, and procuring energy for FirstEnergy's customers who don't select an alternate energy supplier in the states with retail choice.

What sparked your interest in joining the RF Board?

My primary interest was sparked by my two predecessors, Stan Szwed and Jim Haney. Both served on the RF Board and instilled a passion for the reliability and security of the Bulk Electric System when I was fortunate enough to work for them during my career. Another major factor is the members of the current RF Board. I had attended board meetings as an observer in the past and gained an appreciation for the extensive knowledge and diverse background of the Board. It's a great opportunity for me to learn from my board colleagues.

What professional organization and activities are you involved with?

I am a member of the North American Transmission Forum (NATF), IEEE, and EEI's Reliability Executive Advisory Committee and Energy Delivery Advisory Committee. My wife and I have been active with Operation Christmas Child, the Akron-Canton Food Bank, and World Vision. These are activities that we both want to get much more involved with after my professional career is over.

How do you anticipate your past experience will enhance your service?

I'm optimistic my experience in transmission planning and operations, along with my NERC compliance oversight experience in all facets of the Bulk Electric System (BES) including physical/cyber security and fossil/nuclear generation, will enable me to effectively represent the Transmission Sector and be a meaningful contributor to the RF Board.

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

Mitigating existing and emerging threats related to physical and cyber security as well as the reliability issues associated with the changing fuel mix. Collectively, the ERO and industry need to continue to work together to develop new ways to anticipate and respond quickly to these threats and issues. Our collaborative and prompt responses to cold weather preparedness and inverter-based resources are great examples of steps in the right direction.

Align Project Update

About Align

The Align Project, formerly known as the CMEP Technology Project, is a culmination of strategic efforts that began in 2014 with the goal of improving and standardizing processes across the ERO Enterprise. As the ERO Enterprise matures to use a risk-based approach to its regulatory posture for the CMEP, the need to develop a more comprehensive system to manage and analyze information is more acute.

Benefits

The objectives and benefits of the Align Project are:

- Single, common portal for registered entities, enabling consistency of experience
- Real-time access to information, eliminating delays and manual communications
- Improved capability to support the Risk-Based Compliance Oversight Framework
- Enhanced quality assurance and oversight, enabling consistent application of the CMEP
- Improved analytics, including visibility into compliance and reliability risks
- Increased capability to implement audit best practices and processes (planning, fieldwork, reporting, quality assurance)
- Standardization and implementation of common business processes and workflows, enabling increased productivity (estimated 15 percent gain for ERO Enterprise CMEP staff)
- Reduced application costs across the ERO Enterprise (reduce current costs by roughly 29 percent, $320k annual savings)
- Projected investment break-even within five years

Frequently Asked Questions

Align Tool *Frequently Asked Questions (FAQs)* information can be found here.

Align Project Newsletter

Align *Registered Entity Newsletter (May 2019)* can be found here.

Schedule of Functionality by Release

Training

In preparation for the Align Release 1 Go-live in September 2019, all registered entity staff who have responsibilities related to self-reporting, self-logging (if eligible), mitigation processes, and enforcement activities should plan to attend a Release 1 registered entity training. Please see the training dates for all Regions below and plan to attend the session closest to your location. Additional training options, including webinars, short videos, and quick reference cards, will be made available leading up to the September 2019 Go-live.

Release 1 Registered Entity Trainings		
Region	**Training Date(s)**	**Location**
MRO	September 4 September 10	N/A
NPCC	September 11	NPCC Office, New York City, NY
RF	September 10 September 12	Reliability First Office, Independence, OH
SERC	August 13 August 20	SERC Reliability Corporation, Charlotte, NC
Texas RE	August 28	Texas Reliability Entity, Austin, TX
WECC	August 27	Tri-State Generation and Transmission Association, Westminster, CO
	August 29	California ISO, Folsom, CA
	September 5	WECC, Salt Lake City, UT
	September 10	Bonneville Power Authority, Portland, OR
	September 12	Douglas County PUD, East Wenatchee, WA

RF is currently preparing registration information and capabilities through our EventBrite system for the RF Training dates listed above. As soon as registration for the RF Training Dates is available we will communicate this information to our stakeholders and specifically to all Primary Compliance Contacts (PCCs).

Please contact RF Align Change Agent, Ray Sefchik or call (216) 503-0651 with any questions .

Summer 2019 Reliability Resource Risk Assessment

RF performs a seasonal summer resource adequacy assessment based on the data PJM and MISO provide. This article shares some highlights from the MISO, PJM, and RF assessments. For the upcoming summer of 2019, both MISO and PJM are expected to have an adequate amount of resources to satisfy their respective planning reserve requirements. Below are the statistics that support our analysis on outage risk, which concludes that there should not be an issue supplying demand within the RF Region this summer.

PJM Capacity and Reserves

Net capacity Resources[1]	188,942 MW
Projected Peak Reserves	45,738 MW
Net Internal Demand (NID)	143,204 MW
Planning reserve margin	31.9%

The PJM forecast planning reserve margin of 31.9 percent is greater than the PJM planning reserve margin requirement for the 2018 planning year of 15.9 percent. The planning reserve margin for this summer is lower than the 2018 forecast level of 32.8 percent. This is due to a decrease in capacity transfers since OVEC has been integrated into the PJM footprint.

MISO Capacity and Reserves

Net Capacity Resources	141,175 MW
Projected Peak Reserves	22,816 MW
Net Internal Demand (NID)	118,359 MW
Planning reserve margin	19.3%

The MISO forecast planning reserve margin of 19.3 percent is greater than the MISO planning reserve margin requirement of 16.8 percent for the 2019 planning year. The planning reserve margin for this summer is slightly higher than the 2018 forecast level 19.1 percent. This is mostly due to increase in capacity in MISO's market.

RF Footprint Resources

Net Capacity Resources	203,531 MW
Projected Peak reserves	37,986 MW
Net Internal Demand (NID)	165,545 MW
Total Internal Demand (TID)	174,971 MW

Since PJM and MISO are projected to have adequate resources to satisfy their respective forecasted reserve margin requirements, the RF region is projected to have sufficient resources for the 2019 summer period.

Random Generator Outage Risk Analysis

The following analysis evaluates the risk associated with random outages that may reduce the available capacity resources below the load obligations of PJM or MISO. Reports and/or other data released by PJM, MISO or NERC for this same period may differ from the data reported in this assessment due to different assumptions that were made by RF from the onset of the report. This analysis differs from NERC's in that RF uses actual historical GADS data from a rolling 5 year period which provides a range of outages that occur during the summer period. The forecasted maintenance outages used in this analysis are derived from PJM and MISO for the summer months.

The stacked bar charts in Exhibits 1 and 2 are based on forecasted Summer 2019 demand and capacity resource data for the PJM and MISO RTOs. The daily operating reserve requirement for PJM and MISO at the time of the peak demand is also included as a load obligation. The range of expected generator outages is included for scheduled and random outages. The random outages are based on actual NERC Generator Availability Data System (GADS) outage data from May, June, July, August and September of 2014 through 2018.

The committed resources in PJM and MISO are represented by the Resources bar in shades of blue and only include the net interchange that is a capacity commitment to each market. Additional interchange transactions that may be available at the time of the peak are not included as they are not firm commitments to satisfying each RTO's reserve margin requirement.

The firm demand and the demand that can be contractually reduced as a Demand Response are shown in shades of green. The firm demand constitutes the Net Internal Demand, with Total Internal Demand including the Demand Response. The daily Operating Reserve requirement (shown in yellow) is between the NID and DR bars. There are two sets of stacked Demand bars on the chart, one representing the 50/50 demand forecast and one representing the 90/10 demand forecast. For instance, the 50/50 demand forecast projects a 50 percent likelihood that demand exceeds 143,204 MW. The 90/10 demand forecast is a more conservative model, projecting a 10 percent chance that demand exceeds 155,952 MW. Since DR is utilized first to reduce the load obligation when there is insufficient capacity, this part is at the top of the Demand bar. In the event that utilization of all DR is not sufficient to balance capacity with load obligations, system operators may first reduce operating reserves prior to interrupting firm load customers.

Between the Resources bar and the Demand bars is the Outage bar. While scheduled outages during the summer season are generally minimal, there are

[1]Net capacity resources include existing certain generation and net scheduled interchange.

Continued on page 6

Summer 2019 Reliability Resource Risk Assessment

Continued from page 5

scheduled outages planned during the summer that are reflected in the amount of Scheduled Maintenance (colored gray) in the Outage bar. The remainder of the Outage bar represents the entire range of random outages (pink shows 100 percent of the random outages; rose shows less than 100 percent down to 10 percent of the random outages; and red shows less than 10 percent down to 0.1 percent of the random outages on the chart) which occurred during the five-year reference period.

In the following discussion of the random outages, the analysis of random outages exceeding certain reserve margin targets is presented as a probability. These probabilities are not based on a true statistical analysis of the available daily random outage data. Rather than statistical probabilities, these numbers represent the percentage of the daily outages during the five prior summer periods that would have exceeded the reserve margin that is listed. They are discussed as probabilities as a matter of convenience in describing the analysis results.

To the left side of the range of random outages are probability percentages related to the amount of random outages that equal or exceed the amount of outages shown above that line on the Outage bar. Moving from top to bottom of the Outage bar represents an increasing amount of random outages, with a decreasing probability for the amount of random outages. In the PJM chart, the random outages represented by the bar above the 100% point is 6,641 MW. This means that the probability of there being at least 6,641 MW of random generation outages is 100 percent. Similarly, at the 10 percent point, the outages represented by the bar above the 10 percent point is 19,775 MW (6,641 MW + 13,134 MW). There is a 10 percent probability that there will be at least 19,775 MW of outages. As shown by the probabilities and corresponding amounts of random outages, the distribution of random outages is not linear throughout the range of outages observed.

To the right of the Outage bar are the probabilities of the random generation outages that correspond to different levels of demand obligation.

In Exhibit 1, the top of the 90/10 Demand obligation bar for PJM represents TID with operating reserves. The 4% line between the Outage bar and the 90/10 Demand bar represents the probability that there will be an amount of outages that will require Demand Response resources to be utilized. This means that there is a probability of utilizing Demand Response during high demand (90/10).

Exhibit 2 contains the information to perform the same analysis for MISO. The top of the 50/50 demand obligation bar for MISO represents TID with operating reserves. The line between the Outage bar and the 50/50 Demand bar represents a 13 percent probability that there will be an amount of outages that will require Demand Response resources to be utilized. The top of the 90/10 demand obligation with the operating reserves has a 100 percent probability that Demand Response will be required.

Exhibit 1 - 2019 Summer PJM Outage Risk Chart

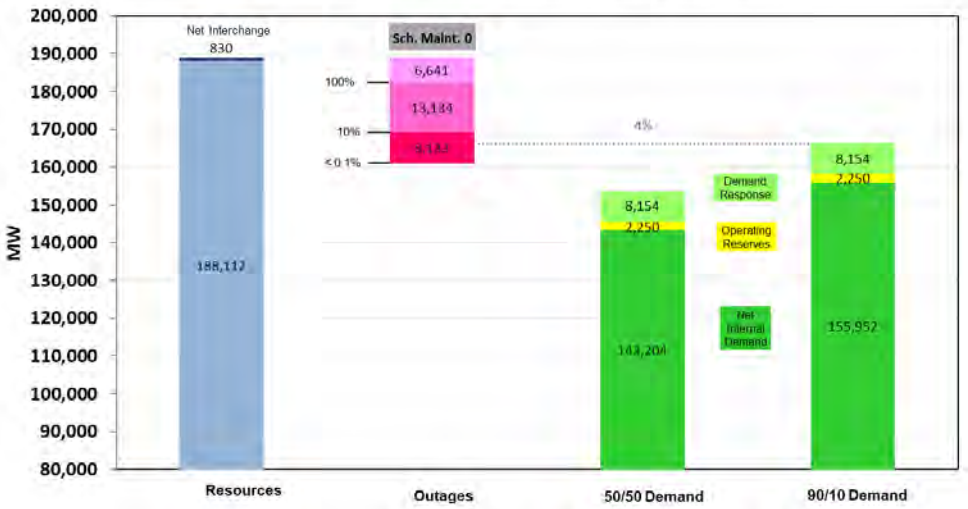
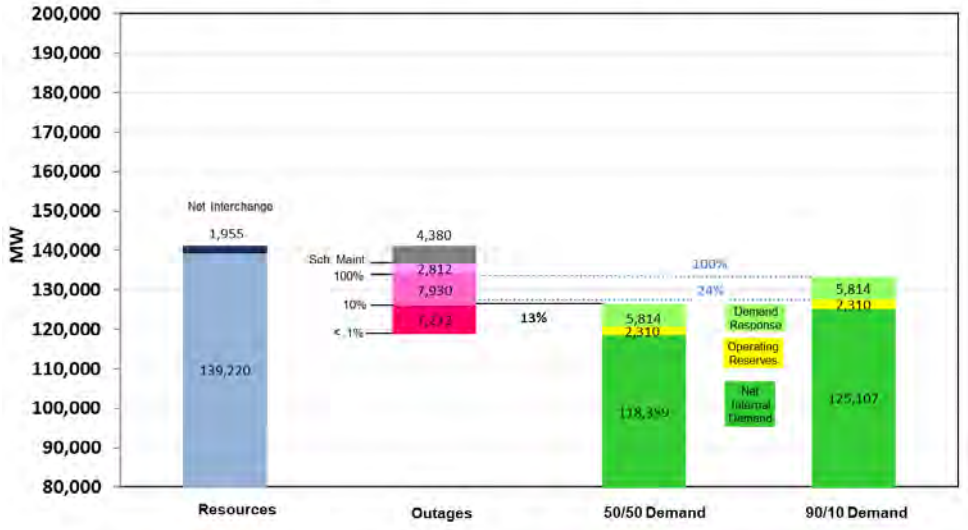


Exhibit 2 - 2019 Summer MISO Outage Risk Chart



Contractor Oversight

By: Kellen Phillips, Principal Analyst

Improving Third Party Management

The use of outside contractors is a common practice by many electric utilities. These contractors are used for numerous tasks, some of which are used in part or whole to meet NERC Reliability Standards. These tasks can range from vegetation management, to Protection System maintenance and testing, to cyber security risk assessments.

While the use of contractors can be beneficial and sometimes necessary, there are some steps to take to ensure their work is done to ensure safe, secure, and reliable operations and meet the criteria specified in the NERC Reliability Standards to mitigate any reliability and compliance risk.

This article outlines some of the common issues that RF has seen with contracted work and shares practices that the entities can integrate into their processes to help improve contractor performance.

Below are some of the issues that RF has observed:

- Lack of an adequate process/controls to review and assess contractor work,
- Incomplete or unclear documentation of the work from the contractor,
- Contractors not adhering to a Registered Entity's testing procedures,
- Contractors with little or no experience in completing the required testing, and
- Lack of proper scheduling to ensure deadlines around contractor work are met.

Some applicable Standards:

PRC-005-6	PRC-019-2	PRC-024-2	PRC-025-2	MOD-026-1
MOD-027-1	MOD-032-1	MOD-033-1	CIP-004	CIP-007
CIP-010	CIP-011	CIP-014		

It is imperative to remember that while the use of independent contractors can be a beneficial tool in getting work completed, their work does not absolve compliance responsibility from the Registered Entity. Registered Entity oversight and the use of internal controls assures the work is performed correctly and helps ensure that reliability requirements are met. In some instances, RF has observed strong controls, including leveraging technology and notifications to help with the oversight and review of contracted work.

The staff at RF has put together internal controls guidance documentation to help entities develop their programs and mitigate these risks. These internal control documents with additional information and guidance will be posted shortly on the www.rfirst.org Knowledge Center.

Three internal controls that are essential to assisting entities when assessing their interaction with contractors are:

Contract (3rd Party) Management:

- Ensure contract accuracy: the expected outcomes, success factors, and timelines.
- Request references from the contractors, or contact neighboring electric utilities to understand their experience with contractors.
- Validate and track contract performance; did the contractor meet all the goals or were there any gaps?

Documentation:

- Did the contractor document *all* of their work (not just the results) to prove that they completed all required activities according to your specifications?
- If possible - processes, reports, etc. should have a standardized format to reduce errors and drive consistency.
- Example: Utilizing a standard template for PRC-005 that includes all of the activities from the Protection System Maintenance and Testing Plan (PSMP) may make it easier to complete in the field and review for accuracy.

Continued on page 8

Contractor Oversight

Continued from page 7

Analysis:

- Establish a process or methodology for reviewing the data.
- Analyze the data according to the process (i.e. is the data producing the desired results or meeting the objective?)
- Communicate the data and results as needed. What did the testing show you? Are any system changes needed?

In Summary:

1. Contract management and entity oversight are critical to mitigate reliability and compliance risks when an entity is engaging contractors. The contracted work should have a clear scope, with specific deliverables andappropriate oversight to ensure that the proper testing is timely and has been completed.

2. Entities need to review the final results with the contractor to ensure all tasks were completed and documented. The testing or documentation should be reviewed with the contractor to address any questions and clarify the data/results. Remember, the entity is ultimately responsible for the work being performed with the help of the contractor and should have a clear understanding of the documentation.

3. Entities should analyze the data provided by the contractor to check for errors and to see if there are any risks to reliability or security.

   a. Do the test results make sense? Ask questions to the contractor. They should be able to explain the results and outcomes and make recommendations if needed based on the work performed.

   b. What is the data telling you? For example, is the accuracy of instrument transformer adequate or is additional maintenance (or a replacement) necessary? Are protection setting changes required?

   c. If you have questions, seek additional help. You can schedule an Assist Visit with RF or ask your peers for assistance.

   d. Having strong analysis controls when reviewing the documentation will help to mitigate compliance risk.

RF will continue to add information to our Internal Controls Knowledge Center and provide more examples where internal controls can mitigate risks and improve overall performance.

Insider Threats - Personnel & Training - Part 3

By: Bheshaj Krishnappa, Principal Analyst

In the previous article, we discussed on how to establish a formal Insider Threat Program management function at your organizations. After the critical step of establishing an Insider Threat Program office with a Senior Designated Official, the next step is Personnel and Training. This aspect involves two areas; (1) hiring and staffing for the Insider Threat Program and (2) conducting employee training and awareness.

1. **Hiring and staffing:**

   Individuals hired for the Insider Threat Program should have a high degree of ethics, professionalism, personal integrity, and the ability to maintain confidentiality. The team may be comprised of permanent and temporary staff. Permanent Staff are generally analysts who specialize in IT, databases, and forensics. The Insider Threat Program analysts can be chosen with experience in incident response, databases, investigations, forensics, auditing, physical and cyber security areas. Furthermore, the analysts skillsets can be enhanced by periodic training on tools and techniques.. Sometimes, if the analyst has shared responsibilities, it is important to isolate the Insider Threat Program duties. As the Insider Threat Program staff will have access to sensitive personnel information, they are expected to maintain a professional ethical behavior and requirements to ensure it should be in place.

   Temporary staff are generally Human Resources, Legal and Psychologists. The temporary staff are called on an as-needed basis to solicit their expertise on individual insider threat cases and they may also participate in periodic Insider Threat Program meetings. The National Insider Threat Task Force Maturity Framework notes that hiring staff for the Insider Threat Program from a broad range of functional areas with multi-disciplinary expertise can increase the effectiveness of the program.

   Depending on the size of the company and the criticality of the identified assets, the staff managing the Insider Threat Program can be derived from existing business units who are already performing IT/Security, Legal, and Human Resource activities instead of hiring and training new staff. In some cases it makes sense to consider hiring external personnel if the subject matter expertise is not available in-house. Keep in mind that external personnel may require Non- disclosure agreements or Memorandums of Understanding to ensure the integrity and confidentiality of tasks involved.

2. **Employee training and awareness:**

   NERC Reliability Standard CIP-004-6 Security Awareness Program and Cyber Security Training Program requirements already mandate periodic and effective security training. Though the NERC Standards do not mandate a specific Insider Threat awareness training, it may be prudent to formally incorporate Insider Threat training modules as a good security practice to increase awareness. In energy critical infrastructure, the challenge of ensuring a reliable Bulk Power System (BPS) involves both physical and cyber areas. Usually the Insider Threat training can be done in one of two ways, a specific role-based training of Insider Threat Program staff, and/or an organization-wide training for all employees. These trainings can alleviate and dispel myths associated with Insider Threat Program in the organization and help to create awareness amongst staff.

The training topics may include

- What is an Insider Threat? Looking at the types of Insider Threats to secure critical assets.
- Insider Threat policies, procedures, and programs
- Employee rights and responsibilities, privacy, hotlines and reporting

There are several free resources available to assist with training personnel on Insider Threats, to deter, detect and mitigate insider threats. The National Insider Threat Special Interest Group has compiled a list of resources on awareness and training that may help establish a training program at your organization. Some of the links are noted below:

- Department of Homeland Security (DHS); Insider Threat Awareness Video
- If You See Something, Say Something -Insider Threat Awareness Video (DHS)
- Insider Threat Awareness Link 1; Link 2
- Center for Development of Security Excellence Video

Continued on page 10

Insider Threats - Personnel & Training - Part 3

Continued from page 9

The Software Engineering Institute at Carnegie Mellon University offers more formal certificate based online and in-person courses on Insider Threats, including: Building an Insider Threat Program, Insider Threat Analyst, Insider Threat Program Manager, and Insider Threat Program Evaluator courses. The book CERT Insider Threat Center's Common Sense Guide to Mitigating Insider Threats, Fifth Edition can serve as a reference for crafting a training program that best suits your organizational needs.

According to the CERT Insider Threat Center, there are five types of insider threat activities:

1. Insider Threat Sabotage.
2. Insider Threat Intellectual Property Theft
3. Insider Threat Fraud
4. National Security Espionage
5. Unintentional Insider Threat

For energy critical infrastructure, IT Sabotage and Unintentional Insider Threat categories are important to focus on. Insider Threat Sabotage is the most sophisticated or technical type of attack, where disgruntled employees/contractors commit harm, usually as a result of unmet expectations or for revenge. Conversely, an Unintentional Insider Threat occurs when a current or former employee, contractor, or business partner who has or had authorized access causes harm without malicious intent.

Most of the unintentional cases are as a result of human error. Unsurprisingly, human performance improvement is a recognized field of work in the energy industry and many activities are occurring in this direction.

The IEEE paper "Unintentional Insider Threat: Contributing Factors, Observables, and Mitigation Strategies" notes that training people to identify cognitive biases and limitations can help people overcome committing errors or judgment lapses. A 2016 Ponemon report notes negligence as #1 cause of insider threats.

This is synonymous with majority of NERC Reliability Standards compliance findings noting that the root causes are due to human error. An effective solution is to educate employees, contractors and business partners by conducting frequent training and awareness programs to reduce unintentional incidents.

Overall, creating a strong training program that focuses on high-risk personnel and high-value assets can help. Such training should also create awareness around Insider Threats and work towards creating a culture of compliance that can promote the reliability and security of the BPS that we all depend on.

References:

https://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_484758.pdf

https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6758854

https://accudatasystems.com/wp-content/uploads/2016/04/whitepaper_unintentional_insider_threat_cost_en.pdf

https://www.forcepoint.com/sites/default/files/resources/files/infographic_insider_threat_negligence_number_one_cause.pdf

https://www.nationalinsiderthreatsig.org/itrmresources/Insider%20Threat%20Awareness%20Training%20Resources%207-19-15.pdf

https://www.forcepoint.com/sites/default/files/resources/files/infographic_insider_threat_negligence_number_one_cause.pdf

https://www.nationalinsiderthreatsig.org/itrmresources/Insider%20Threat%20Awareness%20Training%20Resources%207-19-15.pdf

Source: Ponemon Report (2016)

PJM is studying the potential impacts of carbon pricing on the competitive wholesale energy market to inform the decision makers across the region who are considering climate policies.

Gary Helm, lead market strategist – Applied Innovation, outlined the study for members of the Market Implementation Committee on May 15.

PJM is not proposing to establish a carbon price, Helm said. PJM's interest is in maintaining grid reliability and keeping the markets competitive amid external influences.

Some carbon pricing already flows through the market related to the Regional Greenhouse Gas Initiative, a nonprofit cooperative effort among nine states to reduce greenhouse gas emissions – but it's not significant enough to impact dispatch operations or create cross-border issues, Helm said.

The study will look at a scenario in which a significant carbon price is imposed on a regional or sub-regional level for the 13 states and the District of Columbia covered by PJM, and how that would impact dispatch and emissions.

PJM recognizes the states' responsibility to develop environmental and energy-resource policies. PJM believes the most efficient way to enable state policies aimed at reducing carbon emissions from power plants is to reflect the cost of carbon in wholesale energy market prices.

The study is being conducted in tandem with the work of a new senior task force. The task force will study frameworks that could accommodate states' carbon-pricing policies while mitigating negative spillover effects into surrounding states, while preserving orderly and competitive economic dispatch of generation resources across PJM's 13-state footprint. States' greatest concern is the prospect of "leakage" – when higher-emission generators from regions without a carbon price import cheaper energy into an area with a carbon price, putting lower-emission generators at a disadvantage and defeating the purpose of a carbon price.

The study will review the impacts of a carbon price on PJM's energy and ancillary service markets, both across the entire system and at a sub-regional level. On a sub-regional level, PJM will look at the likely grouping of Delaware, Maryland and New Jersey. Delaware and Maryland already participate in the Regional Greenhouse Gas Initiative, and New Jersey is considering joining.

The review will address the energy market, not the capacity market.

Helm introduced the variables to be used in the study to address leakage, including three border-adjustment approaches: no price adjustment for imports/exports, a one-way adjustment on imports into a carbon-pricing region, and two-way border adjustments.

The base price it will use is the social cost of carbon for 2023, which is $52.79 per ton of carbon dioxide.

The study builds on the work of a whitepaper PJM released in 2017 that explored approaches to carbon pricing.

Carbon pricing also was the subject of the General Session panel at the Annual Meeting May 8. Participating industry experts said PJM's mission of ensuring a reliable, affordable grid will benefit from considering how carbon-pricing policies could be integrated into the competitive market.

Get Control of Yourself!

By: Denise Hunter, Principal Technical Auditor

Welcome to the first in a series of articles focusing on developing a strong internal control program. Our goal with this column is to share information, suggestions, and industry examples to aid in understanding what an internal control program consists of, thus providing insight on how to craft a control program and suggestions to help strengthen existing programs.

An internal control program consists of five components:

- Culture
- Risk Assessment
- Internal Control Activities
- Information and Communication
- Monitoring

Over the last few years, RF has offered ideas regarding possible approaches to addressing the internal control activity components and understanding what an internal control activity is and how to document it. To advance our conversation regarding the internal control program, we now will explore the component of identifying risk and determining appropriate, feasible mitigating control activities.

There are numerous factors that need consideration to properly assess an entity's risk to the BES: organizational structure, compliance history, registration, ERO/RF risk elements, to name a few. The majority of these criteria are unique to the entity, and therefore would be difficult to discuss in a generalized fashion.

The exception is the ERO/RF risk elements. NERC identifies risk elements using data including, but not limited to:

- compliance findings;
- event analysis experience;
- data analysis; and
- the expert judgment of NERC and Regional staff, committees, and subcommittees (e.g., NERC Reliability Issues Steering Committee).[1]

During the 2019 CMEP IP process the ERO identified eight ERO risk elements. RF identified four additional risk elements and expanded on one of the ERO risk elements.

Over the course of the next few newsletters, this series will review the eight risk elements, aiming to provide applicable Standards, industry risk examples and relevant mitigating controls, with detailed insight into one suitable mitigating control for each risk element.

We begin our review with **Improper Management of Employee and Insider Access**. The focus of this risk element is the risk posed by the *human element of security*. Regardless of the sophistication of a security system, there is potential for human error. Entities must identify and manage the risk of how many people have access, both physical and technical, and be aware of the complexity of the tasks employees are asked to perform.

When considering this element during risk assessment, at a minimum, forethought should be given to:

a) Structural access during position changes, terminations, organizational changes, etc.

b) CIP systems and technology access, as outlined within the CIP Standards,

c) computerized spreadsheets and workbooks utilized to perform complex tasks, and

d) all computer systems used to maintain a reliable grid.

The following Standards have been identified as applicable to this risk element:

- Personnel & Training (CIP-005-5)
- Electronic Security Perimeter(s) (CIP-004-6)
- Physical Security of BES Cyber Systems (CIP-006-6)
- System Security Management (CIP-007-6)
- Configuration Change Management
- Vulnerability Assessments (CIP-010-2)
- Information Protection (CIP-011-2)

[1] 2019 ERO CMEP Implementation Plan V2 November 2018, page 7

2019 Risk Elements

Improper Management of Employee and Insider Access
Insufficient Long-Term Planning Due to Inadequate Models
Insufficient Operational Planning Due to Inadequate Models
Spare Equipment with Extended Lead Time
Inadequate Real-time Analysis During Tool and Data Outages
Improver Determination of Misoperations
Inhibited Ability to Ride Through Events
Gaps in Program Execution

Continued on page 13

Get Control of Yourself!

Continued from page 12

However, I feel the risk elements often permeate more than the identified Standards, applying to all areas of the organization.

The CIP Standards noted above focus on incidents regarding security breaches, either physical or technical, and securing cyber information. Ensuring the security of those areas is of the utmost importance, however the risk identified by this element should expand beyond those to areas such as excel workbooks designed to perform complex tasks used for Grid reliability.

A few examples: Facility Ratings (FAC-008-3), Transmission Relay Loadability (PRC-023-4), Generator Relay Loadability (PRC-025-2). Often times excel workbooks are used to ensure consistency while performing these calculations, however access to the workbook, and actual cell calculation information, is not protected.

These workbooks should be:

1) Owned by one position within the department responsible for the function, thereby ensuring only approved changes are implemented,

2) password protected, allowing access to only those personnel that are performing that function, and

3) locked so that cells within the workbook containing 'static' information (i.e. calculations) can't be overwritten.

The final step in addressing the risk elements is to identify the appropriate internal control activities to mitigate the risk. There are a number of internal controls that should be considered when crafting a control activity to mitigate this risk: Access controls, Asset Management controls, Change Management controls, Termination controls, and Segregation of Duties.

The objective and activities (to the right) can assist in crafting a strong Access Control. With the addition of each activity listed above, the breadth and strength of the control increases.

A 'perfect' internal control will never exist, however by identifying the appropriate access levels, and including activities within the control that address personnel movement, the risk of Improper Management of Employees and Insider Access can be mitigated.

This newsletter will be captured on the Internal Controls Knowledge Center, and if you have any questions or areas of an internal control program that you would like answered or addressed, the Knowledge Center contains a link for those submissions.

I look forward to continuing this conversation in upcoming newsletters.

Access Controls

Objective:

The selective restriction of access to a place or other resource.

Control Activities:

Including the following activities will help to strengthen the control activity.

Activity 1	**Controls established for both physical and control system access.**
Activity 2	**Defined access levels established by position.**
Activity 3	**Employee promotions, position changes or termination of employee/contractors initiate a review of access needs.**
Activity 4	**Entity performs periodic reviews of personnel access levels to identified systems to ensure appropriate access is maintained.**
Activity 5	**Changes due to: technology, mergers, acquisitions, infrastructure changes, etc. require a review of all position access.**

The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

CIP Supply Chain Cyber Security Requirements in Depth (Part 2 of 3)

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.

In my Nov/Dec 2018 article, I discussed CIP-013-1, Supply Chain Risk Management, at a high level. I discussed how I think CIP-013-1 is at the same time plan-based, objective-based, and risk-based. In my Jan/Feb 2019 article I provided a suggested structure for a risk management plan. In this article I'll continue what I began in the Mar/Apr 2019 article, which was a detailed look at the supply chain risk management Requirements for CIP-013-1.

I had planned to cover the supply chain changes to both CIP-005-6, Electronic Security Perimeters, and CIP-010-3, Configuration Change Management and Vulnerability Assessments, in this article, but to allow me to get more in-depth I will cover CIP-010-3 in the Jul/Aug issue as the third part of this now three-part article. Please remember that if you choose to adopt any of my suggestions, you must adapt them to your entity's position in the Bulk Electric System, and to your entity's systems and policies.

On the May Reliability and Compliance Open Forum Call, I presented a brief overview of the supply chain Standards which includes a slide with links to relevant documents. The presentation from that call is here.

If you want to participate in these monthly calls, the information is on the Compliance Monitoring page of the RF Website.

Malicious Remote Access

Suppose you're the EMS engineer in charge of your primary control system. One afternoon as you're getting ready to go home, you get a call from the operations supervisor. Some of his operators are having trouble with their control consoles. The mouse associated with each console is not working properly. It seems to be moving the display cursor on its own, and not responding to the actual movements of the mouse. As you're speaking, he reports that a breaker controlled by one of the consoles has just been commanded to open. He asks what can be wrong with the systems, and why his operators have suddenly lost control of BES operations. How quickly can you fix this problem and get his operators back in control?

Huron Lightship, Port Huron, MI - Photo by Lew Folkerth

Is this fiction? No. This is the scenario that actually occurred on December 23, 2015, in Kiev, Ukraine (see *Analysis of the Cyber Attack on the Ukrainian Power Grid* here.) And this is the scenario that I believe motivated FERC to address the ability to control vendor remote access. In this article, I'll discuss how the risk of this scenario can be reduced, and how your response can be designed to quickly remediate an actual incursion.

CIP-005-6 R2 Parts 2.4 and 2.5

In Order 829 at P 51-55, FERC required NERC to develop a Reliability Standard to address the risk of vendor remote access to BES Cyber Systems. The new Standard was to cover both interactive and system-to-system remote access. FERC explained that its concerns included malicious use of stolen credentials, possible compromise of a trusted vendor, and use of a vendor's access to compromise or control a BES Cyber System. FERC also stated that an entity

Continued on page 15

Continued from page 14

should be able to "rapidly disable" remote access connections.

CIP-005-6 includes two new Parts. You are required to have methods "for determining" (Part 2.4) and "to disable" (Part 2.5) active vendor remote access sessions. Let's look at the enforceable language of each Part in detail:

R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in:

Applicable System	Requirements
High Impact BEC Cyber Systems and their associated PCA; and Medium Impact BES Cyber Systems with External Routable Connectivity and their associated PCA	Part 2.4: Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).
	Part 2.5: Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).

Let's look at some important points regarding this language:

1. We can look at these Parts as bringing certain Electronic Security Perimeters (ESPs) into scope. All ESPs that contain a high impact BES Cyber System are in scope. All medium impact ESPs that have at least one Electronic Access Point (EAP) associated with the ESP will also be in scope. Within these in-scope ESPs, all Cyber Assets will be in scope. Remember that if any Cyber Asset is within an ESP that has an EAP, the Cyber Asset will almost certainly have External Routable Connectivity (see *The Lighthouse* from Jul/Aug 2015 available here.)

2. Looking at the Requirements, we see we're dealing with several terms not defined in the NERC Glossary. You may need to incorporate your own definitions of any non-glossary terms into your processes and procedures. If you do so, be careful to use commonly accepted definitions and apply them in a way that makes sense in the context in which they're used and that achieves the intent and purpose of the standard.

3. The scope of these Parts includes all data communications into or out of every in-scope ESP, not just routable network traffic. Dial-up, serial leased line, or other communications can also be construed as "remote access," even if it does not employ a routable protocol.

4. These Parts are silent as to how quickly you must be able to respond to an identified issue. In my opinion, identification of malicious remote access sessions and disabling of such access should be achieved in seconds or minutes, not hours or days. If you doubt this, ask your system operators how long a malicious actor should be allowed to control their systems.

5. While the term "vendor" is defined in the Rationale section of the Standard, remember that this section is considered to be guidance and is not enforceable. Rather than be concerned about the precise definition of "vendor," I recommend that, for these Parts, you disregard the term and provide equal consideration for all communications into and out of an in-scope ESP. This will probably be simpler from a compliance perspective and certainly more effective from a security perspective.

6. These Parts are also silent on recovery. I recommend that your processes include methods of capturing forensic evidence, so you can identify the cause of the incursion and correct the weaknesses that led to it. As any malicious remote access meets the definition of a Cyber Security Incident, your CIP-008 incident response plan should be activated. Make sure the incident response plan has provisions for dealing with cases of malicious or unauthorized remote access. Also, when recovering systems back to normal operating mode your CIP-009 recovery plan may need to be invoked. Ensure it has provisions for these circumstances.

Continued on page 16

Continued from page 15

How can you control remote access in a manner that meets the security objective of Parts 2.4 and 2.5? I suggest a layered approach to this problem:

Identification:

Control of remote access traffic begins with understanding all traffic that crosses the ESP border, including any traffic that bypasses the ESP border such as dial-up or serial communications. You should already have a good handle on this from the existing CIP-005-5 Requirements, but I think it's time to revisit this topic in more depth. You should clearly understand (and document) the need for each type of traffic permitted into or out of the ESP.

What are the endpoints of the traffic, the source and destination, and what service is provided?

Who uses this service, and why is it needed?

Which firewall rules permit this traffic?

How does it contribute to reliability? What would be the impact if the traffic is blocked?

If the far endpoint for this traffic is compromised, can this traffic be used to compromise BES reliability?

All of these questions should be answered and documented for use in the items below.

Categorization:

Once you identify the traffic, you should categorize the traffic based on reliability need. Consider these as possible categories for your traffic:

- Required for operations under all conditions, normal and emergency
  - This traffic will probably include ICCP feeds to your BA, RC, and/or TOP. It will also probably include monitoring and control links between Control Centers and field devices like a substation RTU or a generator DCS.

- Required for normal operations, but may be suspended for emergencies
  - This category might include engineering workstation access into the production network for routine maintenance and configuration. Traffic that is part of a historian system that is not used for situational awareness might also be included here.

- Convenience connections, not necessary but useful for saving time or labor
  - Most Interactive Remote Access probably falls here, such as engineering connections from home to permit after-hours response.

- Other connections
  - In my opinion, there should be no traffic in this category. If it doesn't support operations, and doesn't save time or labor, why is it permitted into or out of the ESP?

Classification:

Classify the traffic by the type of party you're communicating with:

- Internal: Communication is within your entity's networks or within secure communication links between such facilities.

- Registered Entity: Communication is to another Registered Entity (BA, TOP, etc.).

- External Party: Communication is to another party not subject to the CIP Standards. I consider this traffic to be "vendor" traffic.

Prioritization:

Determine which traffic must be kept operational under various conditions. You might develop three conditions of operation: normal conditions (no suspected threat), heightened security (response to a suspected threat), and maximum security (response to a probable or confirmed active threat).

Response Preparation:

There are some actions you can take to proactively reduce your exposure to remote access threats.

- Architecture:

  Your vendors should not have direct access into your ESPs. If a vendor must have remote access, consider giving your vendor access to a test or QA environment rather than the production control systems. To the greatest extent possible, modify your architecture so that only traffic that is absolutely necessary is permitted into the ESP.

Continued on page 17

Continued from page 16

- Network Configuration:

  You should review your network configuration to determine if modifications can increase the isolation of systems that are capable of remote access. For example, it may be possible to restrict the network visibility of a console that is the target of Interactive Remote Access by placing it on its own VLAN internal to the ESP and restricting traffic to and from that VLAN to the rest of the ESP. This type of segmentation can be valuable in increasing security, but be careful that it doesn't disrupt operations.

- Simplification:

  There may also be opportunities to prevent traffic from crossing the ESP boundary. Services such as Active Directory or network printing could be moved to dedicated devices within the ESP to prevent that traffic crossing the ESP boundary. Analyze this type of change carefully to make sure you are actually improving overall security.

- Security Appliances:

  You may be able to incorporate security systems such as a Security Information and Event Management system or Intrusion Detection System into your remote access protections. Remember, though, that you are after very fast response times and there may not be time to run reports or do extensive analysis.

Response Planning:

Once you know your traffic and have optimally configured your networks, you should plan your response scenarios. At a minimum, you must be able to turn off access to any traffic classified as "vendor" traffic above. A good way to organize the response is to incorporate the prioritization levels identified above. Your target here is to get maximum improvement in security for a minimum in response time. To me, this indicates the need for pre-planned and pre-tested configuration changes that can be implemented with minimum risk to reliability.

These configuration changes should be manually-initiated automated processes so that manual processes don't slow the response or introduce errors in the network configuration. In planning for this type of response, be sure to consider your change control processes.

You don't want to have a required change approval slow down your response to an emergency. Test your automated processes thoroughly. The goal is to improve reliability, but these processes could also have unintended consequences if not properly vetted.

Training and Exercises:

Ensure all personnel who will be responsible for recognizing and reporting instances of malicious or unauthorized remote access are trained in these skills and that their training stays fresh. Ensure the personnel who are to receive these reports are confident and proficient in their roles so they can respond quickly and properly to any identified incursion. Frequent exercises will help with this.

How you detect a remote intrusion and how you disable any such detected access will depend greatly on your position in the BES, on the systems you use, and on your personnel. While I don't have specific advice for detecting and disabling malicious connections that defeat your protective measures, I do believe the planning and preventive actions I've described above will help.

Requests for Assistance

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

Feedback

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

I may be reached here.

In the Industry

NERC Announces Resources Sufficient to Meet Summer Peak Demand in Most Areas

NERC's 2019 Summer Reliability Assessment found that projected resources are at or above the levels needed to satisfy summer peak demand under anticipated weather. The Assessment concluded the landscape for summer 2019 is similar to last years. However, the continual transformation of the resource mix presents opportunities and challenges as the operating characteristics continue to diversify. A few findings include:

- ERCOT anticipates Energy Emergency Alerts may be needed to address resource shortfalls during periods of peak demand because its anticipated summer reserve margin remains low and has dropped from 10.9 percent in 2018 to 8.5 percent in 2019.

- All other areas exceed reference margin levels and have sufficient electricity supply resources for anticipated conditions.

The full report is available here: 2019 Summer Reliability Assessment

Brian Slocum Appointed to Advisory Board for the Michigan Intelligence Operations Center for Homeland Security

Brian Slocum, Vice President of Operations for ITC Holdings, has been appointed to succeed Michael Arthur Bruggeman on the Advisory Board for the Michigan Intelligence Operations Center for Homeland Security. Mr. Slocum will represent residents of the state not connected to law enforcement, for a term expiring April 11, 2023.

The Advisory Board for the Michigan Intelligence Operations Center for Homeland Security collects, evaluates, collates, and analyzes information and intelligence and then, as appropriate, disseminates this information and intelligence to the proper public safety agencies so that any threat of terrorism or criminal activity will be successfully identified and addressed.

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:

- ERO Enterprise CMEP Practice Guide: Implementation of "Annual" and "Calendar Month(s)" in the Reliability Standards
- CMEP Practice Guide, BES Cyber System Information
- Implementation Guidance on CIP-013-1, R1, R2 – Supply Chain Management (NATF), which is a revised version of a previously non-endorsed Implementation Guidance document.

Reliability Standard Audit Worksheets Posted

NERC posted the following new Reliability Standard Audit Worksheets (RSAWs) on the RSAW page under the heading "Current RSAWs for Use."

- PER-003-2 – Operating Personnel Credentials - applies to Balancing Authorities, Reliability Coordinators, and Transmission Operators. The standard becomes effective July 1, 2019.
- TPL-007-3 – Transmission System Planned Performance for Geomagnetic Disturbance Events - applies to Generator Owners, Planning Coordinators, Transmission Owners, and Transmission Planners.

Lessons Learned Posted

NERC posted three new lessons learned on the Lessons Learned page. The new lessons learned address the following topics:

- Automatic Capacitor Operations along Radial Feed Result in Load Shed
- Enhanced Alarming Can Help Detect State Estimator and Real-Time Contingency Analysis Issue
- Telecom Provider Failure Induced Loss of ICCP from Regional Neighbors

Other Resources Posted

NERC has posted the following additional resources:

- NERC has posted the recording and slide presentation for the March 21, 2019 Project 2018-03 – Standards Efficiency Review Retirements webinar.
- The slide presentation and streaming webinar for the April 18, 2019 Project 2018-04 – Modifications to PRC-024-2 webinar have been posted.
- The slide presentation and streaming webinar for the April 24, 2019 Project 2016-02 – Modifications to CIP Standards Virtualization and Future Technologies: Case for Change webinar have been posted. NERC has posted the slide presentation and webinar recording for the April 30, 2019 Violations Themes webinar.

Notable FERC Issuances

In March, FERC issued the following:

- On March 28, 2019, FERC issued a letter order accepting NERC and WECC's joint petition (filed March 9, 2018) and supplemental petition (filed February 11, 2019) for the approval of the retirement of regional Reliability Standard PRC-004-WECC-2 – Protection System and Remedial action Scheme Misoperation. The retirement will be effective January 1, 2021.

In May, FERC issued the following:

- On May 10, 2019, FERC issued a the letter order accepting NERC and WECC's joint petition (filed March 6, 2019) for the approval of Regional Reliability Standard IRO-006-WECC-3 – Qualified Path Unscheduled Flow (USF) Relief in Docket No. RD19-4-000. Regional Reliability Standard IRO-006-WECC-3 will become effective on October 1, 2019.

FERC's issuances can be found here.

Notable NERC Filings

In March, NERC filed the following:

- On March 29, 2019, NERC filed with FERC its 2019 NERC Standards Report, Status and Timetable for Addressing Regulatory Directives in Docket No. RR09-6-003. The annual report is in accordance with Section 321.6 of the NERC Rules of Procedure.

In May, NERC filed the following:

- On May 15, 2019, NERC submitted to FERC a compliance filing, consisting of the unaudited report of the NERC budget-to-actual spending variances during the preceding quarter, filed under Docket No. FA11-21-000. This compliance filing was submitted in accordance with FERC's January 16, 2013 Order, which approved a settlement agreement between the FERC Office of Enforcement and NERC, related to findings and recommendations arising out of its 2012 performance audit of NERC.
- On May 16, 2019, NERC submitted to FERC a request to advance funds from its Operating Contingency Reserves to support the dissolution of Florida Reliability Coordinating Council Inc.'s Regional Entity Division in Docket No. RR19-4-001.
- On May 21, 2019, NERC submitted to FERC a petition for the approval of proposed Reliability Standard CIP-003-8 - Cyber Security – Security Management Controls. The proposed Reliability Standard addresses FERC's directive from Order No. 843 to develop modifications to the standard to mitigate the risk of malicious code that could result from third-party transient electronic devices for low impact BES Cyber Systems. At this time, the petition remains un-docketed by FERC. NERC will update the docket number on its website when it is assigned.
- On May 28, 2019, NERC submitted to FERC the *Cyber Security Supply Chain Risks: Staff Report and Recommended Actions* report. The submission and report are available here. NERC submitted this report to FERC in accordance with FERC's directive in paragraph 31 of Order No. 850. The report was filed in Docket No. RM17-13-000 at FERC.
- On May 30, 2019, NERC and WECC submitted to FERC a joint petition for the approval of proposed Reliability Standard IRO-002-6 Reliability Coordination – Monitoring and Analysis, which reflects the addition of a regional variance containing additional requirements applicable to Reliability Coordinators providing service to entities in the Western Interconnection. At this time, the petition remains un-docketed by FERC. NERC will update the docket number on its website when it is assigned.

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:

Project 2016-02-Modifications to CIP Standards	Comment Period	05/30/19 - 06/28/19

Recent and Upcoming Standards Enforcement Dates	
July 1, 2019	PER-003-2 – Operating Personnel Credentials TPL-007-3 – Transmission System Planned Performance for Geomagnetic Disturbance Events (Requirements 1 and 2)
January 1, 2020	CIP-003-7 – Cyber Security – Security Management Controls; PRC-026-1 – Relay Performance During Stable Power Swings (Requirements 2-4); PRC-026-1- Relay Performance During Stable Power Swings (Requirements 3-4); TPL-007-3 – Transmission System Planned Performance for Geomagnetic Disturbance Events (Requirements 5, 5.1, 5.2, 9, 9.1, and 9.2)
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	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.

Watt's Up at RF

RF Adopts Consolidated Hearing Process

On May 15, 2019, RF's members voted to adopt the Consolidated Hearing Process for contested enforcement matters pursuant to the revised NERC Rules of Procedure, Section 403.15 (effective July 19, 2018).

Under the Consolidated Hearing Process, the Hearing Body will consist of three NERC Board of Trustees representatives (chosen among those trustees not serving on the NERC Board Compliance Committee), and up to two Hearing Body members chosen by the Region (RF).

Under RF's prior process, the RF Board Compliance Committee served as the Hearing Body pursuant to the Board's Amended and Restated Bylaws. On March 14, 2019, the RF Board endorsed proposed bylaw revisions for approval by RF members.

These proposed revisions removed the provision providing that the Compliance Committee will serve as the Hearing Body and instead provide for adopting the Consolidated Hearing Process. The members approved these revisions during a Special Meeting of the Members held in May, 2019.

Under the Rules of Procedure, the Consolidated Hearing Process will become effective six months from the date RF provides notice to NERC that it will adopt the Consolidate Hearing Process. RF is in the process of working with NERC to file its bylaw changes.

RF's New Sampling Process for Verifying Mitigation Complete

In furtherance of implementing a risk-based Compliance Monitoring and Enforcement Program, and in accordance with NERC guidance to the Regions, RF is implementing a sample-driven approach for verifying completion of mitigation associated with minimal risk noncompliances processed as Compliance Exceptions.

While RF was already sampling mitigation related to self-logged noncompliances, RF will now sample mitigation associated with noncompliances processed as Compliance Exceptions for purposes of verification. Under the new process, RF will continue to verify completion of mitigation associated with noncompliance resolved through the Find, Fix, and Track (FFT) disposition type and through Settlement Agreements.

Entity Obligations Under the New Process

Under the new process, an entity's obligation to submit mitigation and complete mitigation milestones and activities does not change. This must be done for every noncompliance. And, entities must continue to submit a certification of completion of mitigation and *retain* evidence in accordance with current data retention requirements. However, entities will *submit* evidence of mitigation completion only if RF requests evidence for that noncompliance.

How RF will Implement the Process

On a quarterly basis, RF will identify a statistical sample of Compliance Exceptions posted with NERC in the previous quarter. RF will then request evidence from the entities in order to verify that mitigation was complete for the mitigation associated with that sample of Compliance Exceptions.

The sample will be partially random, but RF also has discretion to modify the sample pursuant to a risk-based evaluation. For example, RF will ensure it verifies mitigation complete at least once every calendar year for each applicable entity.

These changes should lighten the administrative burden of both RF and the entities so that they can focus less on minimal risk matters and more on addressing and preventing serious risk matters. RF welcomes entity questions about changes to the mitigation verification process.

If you have any questions, please contact Kristen Senk, Managing Enforcement Counsel or Mike Hattery, Associate Counsel.

FBI Citizens Academy

Bheshaj Krishnappa recently graduated from the FBI Citizens Academy class of 2019. The Citizens Academy provides an opportunity for the FBI Cleveland Division to build, develop and strengthen relationships in the communities of Northern Ohio from Toledo to Youngstown.

The FBI Citizens Academy includes eight consecutive evening sessions and a Range Day at Camp Perry, where candidates can explore different firearms. The program covered local FBI divisions' activities on white collar crime, health care fraud, public corruption, transnational cybercrime, counter intelligence, violent gangs, bomb threats, undercover operations, domestic terrorism among other topics. Every year Citizens Academy candidates are selected from a pool of business, religious, civic, and community leaders.

Bhesh Receiving his FBI Citizens Academy Graduation certificate from FBI Special Agents in Charge and Assistant Special Agents in charge at FBI Cleveland Office on May 23rd, 2019.

RF Hosts Registered Entity CORES Pilot/Testing Session

The Centralized Organization Registration ERO System (CORES) Technology Project is progressing according to plan and is scheduled to launch in July of 2019. The ERO will provide multiple training opportunities and an FAQ document has been posted to the CORES project page. CORES combines the registration functions currently managed in OATI – webCDMS, Guidance – CITS, and CRATS into a consolidated registration system. CORES is anticipated to launch the week of July 15, 2019, with multiple training opportunities to be provided by the ERO. On May 14, 2019, RF hosted the first Registered Entity CORES Pilot-Testing Session for stakeholders. This Pilot/Test session served as an opportunity for our stakeholders to be among the first to see and use the new system, and learn about the new efficient, enhanced registration processes. After a step-by-step demonstration of the tool by NERC staff, participants were invited to conduct User Acceptance Testing and asked to provide feedback.

NERC and RF staff were on hand to conduct and assist with the testing. The testing session was done using a system (staging) test environment and included registration test cases and scenarios that included:

- Registering, deactivating, and updating an entity functional registration
  Creating, updating, and deleting contacts
- Entering parent company/affiliate information, and
- Submitting functional mapping information.

Altogether, 15 participants from 13 Registered Entities participated in this pilot and a number of issues or enhancements were identified during the session. The feedback and suggestions provided to NERC and Regional registration staff were extremely helpful and further benefit the development of the tool since they can be addressed prior to production and roll-out to allow for a more successful release.

RF would like to extend our sincere thanks and appreciation to all of the participating Registered Entities for their time and efforts during this Pilot session. Your candid feedback and suggestions will help us develop the best product possible to make the registration process more useful and efficient for NERC, Regions and Registered Entities. We could not do this without your assistance.

If you would like to learn about more about the new CORES technology project and registered entity training, please be aware of the following upcoming Registered Entities training opportunities or go to the CORES website for additional information.

Pre-release entity training schedule:

- To date, NERC has posted several ERO Portal and CORES training videos to the CORES project page. Additional training videos are in the works and will be made available as they are completed.
- CORES WebEx training and Q & A sessions with ERO Registration Staff will be offered in July - August 2019. More information to follow.

Post-release entity training schedule:

- In-person NERC training in Atlanta may be offered. Dates yet to be determined.
- Additional ERO WebEx training sessions will be held in July-August (dates to be announced shortly)

If you have questions about the CORES project, please contact Bob Folt.

CORES
CENTRALIZED ORGANIZATION REGISTRATION ERO SYSTEM

RF Spring Workshop

RF recently held our annual spring workshop. Rob Eckenrod, Vice President & General Counsel of RF, opened the workshop with a keynote address to the approximately 210 attendees.

Erik Johnson, Manager of Entity Development at RF, presented on proposed changes to Appendix 5A of the NERC Rules of Procedure. Appendix 5A governs registration and certification activities and Erik covered the potential changes to the triggers that require an entity to go through the certification review process, as well as additional changes in the overall process.

NERC's Ryan Stewart discussed how the CORES tool development impacts an entity's day-to-day organizational registration activities. The discussion included benefits of CORES implementation, work completed to date, next steps, industry engagements, training, and how you can get involved.

Ray Sefchik, Director of Reliability Assurance at RF, provided an update on the ERO Enterprise Align Tool project, including the current status of important milestones, training information, and the business readiness plan.

After lunch, Sandra Revnell, Compliance Coordinator for Wolverine Power Cooperative, presented on the process and use of straight-forward internal controls processes and tools, focusing on successful implementation at small and medium-size entities.

Max Reisinger and Tom Scanlon, Counsel at RF, provided an update on recent violation trends with a focus on the most violated Standards and Requirements. A panel of RF Registered Entities from ITC, PJM, and DTE Energy discussed strategies to address and help prevent a lack of awareness of the CIP Standards, one of the themes identified in RF, SERC, and WECC's CIP Themes Report.

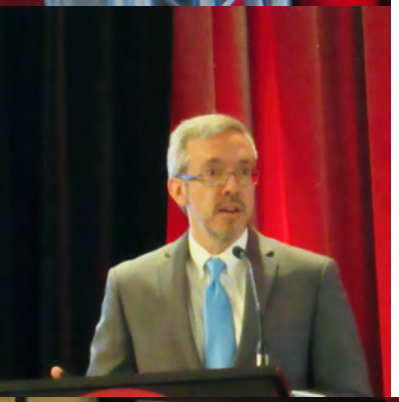
They discussed how to spot the warning signs of potential compliance fall downs, how to stay abreast of the constantly evolving technology, threats, and rules in cybersecurity; and how to leverage your relationship with regulators and industry peers to explore, develop, and implement best practices.

CIP Standards Drafting Teams members Jordan Mallory, Heather Morgan, and Matt Hyatt provided an update on virtualization technology and how it is being addressed within the revisions to the CIP Standards.

Continued on page 24

Watt's Up at RF

Continued from page 23



Day one of the workshop concluded with Kellie Anton, Senior Analyst at RF, providing an overview of the Human Performance Community of Excellence and its objectives, the new RF Human Performance website , and the goals and agenda of the RF Human Performance Workshop and how it complements the NERC Human Performance Conference.

Day two of the workshop consisted of separate events for the Compliance Users Group (CUG) and the Critical Infrastructure Protection Committee (CIPC) to provide information and gain feedback from their members. A Social Hour was held on Wednesday after the CUG and CIPC meetings enabling networking and conversations with both the RF staff and individuals from across the region.

During the first session of day three, RF's Denise Hunter, Principal Technical Auditor, highlighted internal controls and developing an internal control program.

Don Urban, rincipal Analyst at RF, provided a summary of plant winterization efforts from 2018-2019. Don described the amount and type of new generating facilities selected for RF winterization site visits, and the RFI process for gathering and analyzing information for existing and new generating facilities. He also discussed cold weather-related issues which warranted follow-up, including Recommendations, Best Practices and Lessons Learned.

Nathan Case of Amazon provided an overview of cloud services architecture and security when using cloud-based services. He also discussed the shared responsibilities for securing cloud-based services and how the native AWS architecture and security fit into various regulatory and compliance frameworks.

The workshop concluded with Mark Hegerle, Director, Division of Compliance, Office of Electric Reliability at FERC, providing a FERC regulatory update. Mark discussed how the world has changed since reliability regulation began in 2005, how FERC is adapting to changing reliability risks and what we should be thinking about now so we are ready for coming challenges.

We were honored to have such an impressive array of speakers join our team and appreciate all those in attendance. Based on your feedback, we will continue to offer both our Fall and Spring workshops and will do our best to schedule these around other events and on a Tuesday through Thursday in quality venues that can accommodate our needs. Additionally, we are always seeking suggestions and ideas on future topics!

Watt's Up at RF

Homeland Security Active Shooter Training

On May 21, 2019, Michael McMasters, Protective Security Advisor from the U.S. Department of Homeland Security, came to RF to conduct Active Shooter Training. RF staff was advised on how to be alert for suspicious individuals and what to do should an active shooter situation occur. It was an eye opening and informative training for all staff. For more information and online training click here.

RF EASA Hosts NERC EA for Cause Analysis Training

ReliabilityFirst's Events Analysis and Situational Awareness (EASA) Department hosted Rick Hackman and Ed Ruck from NERC Events Analysis (EA) for Cause Analysis Training on June 11th. The training covered different processes to analyze events that occur on the BES. RF looks forward to additional industry collaboration opportunities while analyzing events.

RF Transmission Performance Subcommittee Update

The RF Transmission Performance Subcommittee hosted a joint meeting with the Protection Subcommittee in May. This meeting included several technical presentations, including:

Leslie Krawczyk (RF): Last Summer Performance

Scott Goodwin (MISO): Expected Performance this Summer

Stan Sliwa (PJM): Expected Performance this Summer

Ray Mason (RF): Expected Performance in 2023 and Load Modeling in Light Load Cases

Thompson Adu (MISO): Battery Storage

Scott Baker (PJM): Battery Storage

Justin Michlig (MISO) and Stan Sliwa (PJM): Geomagnetic Storms and NERC Reliability Standard TPL-007

The Subcommittee has been working on the TPS Procedure Manual and also is establishing a Distributed Energy Resources (DER) Survey Task Force.

That task force will survey all the Transmission Owners participating in the TPS to gauge their knowledge and activity with DERs and the extent to which there may be risks to the BES associated with DERs.

They will also hold a DER Workshop on November 5, 2019, where all TPS members are to be prepared to discuss their knowledge and activity with DERs and the extent to which there may be risks to the BES

RF Holds Short Circuit Modeling Workshop

ReliabilityFirst recently held its first ever Short Circuit Modeling Workshop. In attendance were over 60 participants representing 37 different companies. This was a highly technical event covering modeling procedures and techniques as well as the software packages used to model the system and perform analysis. The workshop provided a great opportunity to meet counterparts at neighboring utilities, share practices and experience. Representatives from PJM, SERC, NPCC and NYISO presented the process they each use to assemble their models and some of the tools used for validation.

AEP shared their efforts to capture the impact of planned outages on the protection system to help identify risks and vulnerabilities under these conditions in the operational planning time horizon.

EPRI discussed tools they have developed that will help with wide-area protection coordination studies and model validation. Participants were able to interact face to face with software vendors to discuss issues they were facing and to receive additional instruction on the functionality of various features.

Watt's Up at RF Save The Date

Protection System Workshop for Technical Personnel
August 13-14, 2019

ReliabilityFirst is hosting its fifth annual protection system educational workshop for technical personnel on **August 13-14, 2019** at our office in Cleveland, OH. The focus this year will be on "**Asset Management Tools, the future of Managing Protection System Data**."

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**

This is a highly interactive workshop with the attendees providing ideas, suggestions, and stories for the benefit of everyone. There is no fee to attend this workshop and it is open to anyone interested. Should you have any questions, please contact Thomas Teafatiller.

Register Here

Participation will be limited to the first 85 people!

Human Performance Workshop
August 14-15, 2019

ReliabilityFirst is hosting a human performance workshop beginning on **August 14 (noon to 5:00) through August 15 (8:00 a.m. to noon) at our office in Cleveland, OH**. The topic for this year's workshop is **"Creating (and Maintaining) a Culture that Promotes Human Performance"**.

This workshop will focus 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. This workshop will begin immediately after our annual Protection Systems Workshop for Technical Personnel.

Intended Audience

- **Substation and transmission maintenance**
- **Protection and controls**
- **Operations control rooms including tools support personnel for EMS, SCADA, etc.**
- **Asset design groups (substation, transmission)**
- **Asset management groups**
- **Others interested in these topics (e.g., leaders)**

This is a highly interactive workshop with the attendees providing ideas, suggestions, and stories for the benefit of everyone. There is no fee to attend this workshop and it is open to anyone interested. Should you have any questions, please contact Jeff Mitchell or Kellie Anton.

Register Here

Participation will be limited to the first 85 people!

Fall Workshop
October 1-3, 2019

ReliabilityFirst is hosting our annual Fall Workshop in Cleveland, Ohio.

The Reliability portion, on Oct. 1, will focus on the rapidly changing resource mix including related risks and compliance implications.

To further our role in securing the reliability and security of the bulk power system, we are excited to bring together industry experts on this essential and evolving topic.

In many ways, our Region is at the epicenter of this issue with baseload retirements, the rise in natural gas generation, and our work with multiple Reliability Coordinators.

We look forward to facilitating a multi-perspective discussion for our entities to enhance understanding and improve coordination and reliability across our Region.

Calendar of Events

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

Date	RF Upcoming Events	Location
August 13-14	Protection System Workshop for Technical Personnel	Cleveland, OH
August 14-15	Human Performance Workshop	Cleveland, OH
August 21	RF Board of Directors Meeting	Louisville, KY
August 22	RF Board of Directors Meeting	Louisville, KY
October 1-3	RF Fall Workshop	Cleveland, OH

Industry Events:

Date	Industry Upcoming Events
June 18-19	NERC/NATF Modeling Workshop (Novi, MI)
June 20	FERC Open Meeting
June 27	FERC Technical Conference regarding reliability of the Bulk-Power System (Docket No. AD19-13-000) Washington, DC; Free Web Cast

Public Service Commission of Wisconsin Approves Largest Utility Scale Solar Project in Midwest

The Public Service Commission of Wisconsin approved the building of two utility-scale solar electric generation projects that will more than quadruple the state's solar capacity.

The Two Creeks solar generation facility will have a capacity of 150 MW in Manitowoc and Kewaunee Counties. The Badger Hollow solar generation facility will have a capacity of 300 MW and will be located in Iowa County. Once completed, the two projects will produce renewable energy in an amount equivalent to what 120,000 Wisconsin households use in a typical year.

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