Issue 2
2019 March/April

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,

Spring is in the air and with spring comes new changes and initiatives. One of these is the ERO Enterprise Align project, a major effort that will better align tools and processes across the ERO Enterprise, which we provide an update on in this newsletter. This issue also includes helpful articles on supply chain management; creating an effective Insider Threat Program; and a summary of recent ERO Lessons Learned on drone usage and substation fires.

We also have recaps of two recent ReliabilityFirst events: First, during the 2019 Innovation Awards and Retreat, Bhesh Krishnappa won an award for the Cyber Resiliency Metrics Project (congratulations Bhesh!), and staff workshopped their innovative projects with the management team and outside experts. Additionally, on April 18, ReliabilityFirst hosted the Northeast Ohio Operational Excellence Forum, which focuses on sharing continuous improvement methods among different companies and industries in the region.

I will close by congratulating Gary Campbell, former Manager of Compliance Monitoring for the Operations and Planning Standards, on his recent retirement. Gary has worked for ReliabilityFirst since its inception and has contributed a great deal to our organization. Gary, you will be missed, and enjoy your retirement!

Forward Together,

Tim

Align Project & Tool Development Update

By: Ray Sefchik, Director Reliability Assurance and Monitoring

The ERO Enterprise continues development of the new **Align Tool**, formerly known as the CMEP Technology Tool. As a reminder, the goals of this project are to:

- Better align the business processes of NERC and the Regional Entities
- Improve documentation, sharing, and analysis of compliance work activities
- Make CMEP activities more efficient and effective across the ERO Enterprise
- Provide deep and broad views of reliability across the ERO Enterprise, leading to new insights into data-informed reliability risk management

The ERO strategies to develop and implement the **Align tool** include a strong Change Management program as defined below.

Current activities include the development (design/build phase) of Enforcement related process within the tool including;

- Self Reports,
- Self-Logging,
- Enforcement processing of Possible Non-Compliances, Compliance Exceptions,
- Find/Fix/Track,
- Dispositions,
- Settlement,
- Mitigation Plan Creation, and
- Tracking

ReliabilityFirst will continue to update our stakeholders on the progress of the **Align Tool** development throughout the year.

Updates and details about the Align Tool Project can be found on the ERO website here.

If you have questions or concerns you can contact Ray Sefchik.

An effective Change Management program is critical to enabling NERC to address the people-related risks and drive adoption of the new CMEP tool and processes.

Change Measurement
Stakeholder Engagement
Training & User Support
Communications

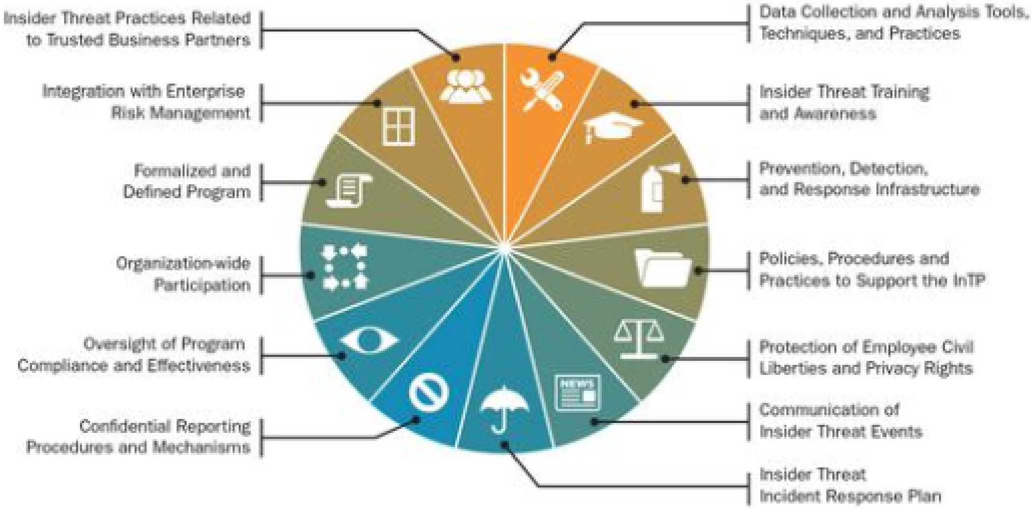
- **Change Measurement** - Facilitate periodic Change Readiness Assessments to measure stakeholder readiness for the adoption of the CMEP tool. Use the output to continue tailoring the activities needed to prepare stakeholders for change.
- **Stakeholder Engagement** - Assess how the project will impact stakeholders and leaders. Engage ERO Enterprise leadership and provide support through a Change Agent Network to reach dispersed stakeholders.
- **Communications** - Establish a communications plan designed to send the right message to the right audiences through the appropriate channels. Develop communications plans to help engage and prepare for change through Targeted Outreach.
- **Training & User Support** - Facilitate a Training Needs Analysis and conduct process and system training to prepare stakeholders with the right skills to perform their jobs.

Insider Threats Program - Part 2

By: Bheshaj Krishnappa, Principal Analyst

In Part 1 of the Insider Threat management series, we learned about the prevalence of insider threats, statistics, and how insider threats can impact the security of the Bulk Electric System. Next, we will learn about the components of an Insider Threat Program and insights on how it can be implemented in our industry.

According to the Software Engineering Institute at Carnegie Mellon University, there are 13 key components of an effective Insider Threat Program. These 13 components include organization-wide participation, protection of employees' civil liberties, confidential reporting procedures, and integrated data collection and analysis.

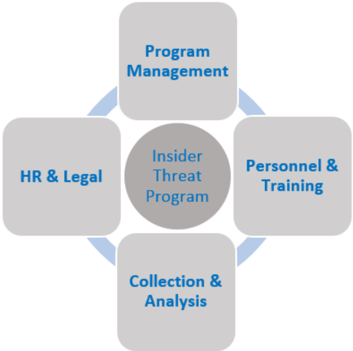

Insider Threat Practices Related to Trusted Business Partners
Integration with Enterprise Risk Management
Formalized and Defined Program
Organization-wide Participation
Oversight of Program Compliance and Effectiveness
Confidential Reporting Procedures and Mechanisms
Data Collection and Analysis Tools, Techniques, and Practices
Insider Threat Training and Awareness
Prevention, Detection, and Response Infrastructure
Policies, Procedures and Practices to Support the InTP
Protection of Employee Civil Liberties and Privacy Rights
Communication of Insider Threat Events
Insider Threat Incident Response Plan
NEWS

These 13 components can be divided into four categories to more easily assess an Insider Threat Program:

- Program Management
- Personnel and Training
- Collection and Analysis
- Human Resources and Legal

In the upcoming series of newsletters, we will discuss these four areas in detail. In this article, we will discuss the first category, Insider Threat Program Management.

Insider Threat Program Management



Most registered entities should already have a CIP Program Management office or at least an identified CIP Senior Manager who is responsible for managing the NERC CIP program. It may make sense to include the Insider Threat Program management under the CIP Program management office, as critical infrastructure protection responsibility falls there. Depending on the entity's organizational structure, an entity may choose to include the Insider Threat Program under its existing corporate cyber and physical security department, or to establish a separate department specifically for Insider Threat management.

CIP-003-6, Requirement 1 requires entities to document and implement cyber security policies that collectively address physical and cyber security of critical assets, access controls, and information protection. The Insider Threat Program and its components go hand-in-hand with many of the CIP requirements an entity may be already complying with. An entity's senior CIP manager can play a critical role to establish an Insider Threat Program within the organization.

Insider Threat Program management includes the following key activities:

1. Establishing a formal Insider Threat Program

   According to the 2019 Insider Threat Program Maturity Model Report, it is important to obtain organizational support and buy-in from senior management to establish an Insider Threat Program, and to appoint a designated senior official to manage the program. In order to achieve this, it is helpful to engage senior management, HR, Legal, IT, Security and key personnel such as department heads from the start and on an ongoing basis as needed.

2. Drafting an Insider Threat Program policy.

   A clearly drafted Insider Threat Program policy can add structure to the whole program. This policy can leverage existing CIP policies covering cyber and physical access controls, confidentiality of information, acceptable use, and data handling. It is also helpful to leverage the existing National Insider Threat Task Force (NITTF) Insider Threat Program Maturity Framework to incorporate best practices. This framework can help measure the effectiveness of the Insider Threat Program at a later date. The NITTF's National Insider Threat Policy and Carnegie Mellon University's Common Sense Guide to Mitigating Insider Threats, Fourth Edition are additional resources with valuable insights for drafting a customized Insider Threat Program policy.

Continued on page 4

Insider Threats Program - Part 2

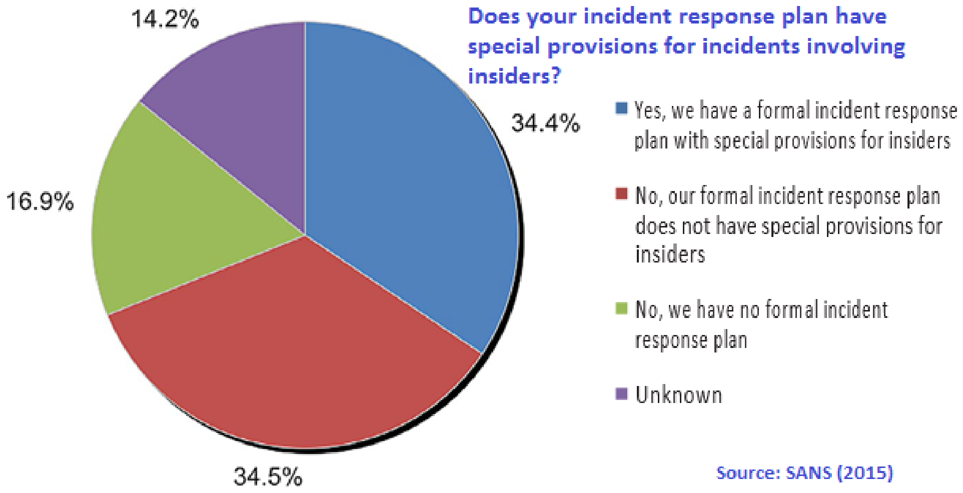
Continued from page 3

3. Critical Asset Identification

   Entities subject to the CIP Standards should have already identified the BES related digital, cyber and physical critical assets they need to protect. However, for insider threats, the critical asset identification can be much broader, and can also include financial information, strategic information, and customer financial information. After identifying the scope of critical assets to protect, the next step is to identify the potential insider threats associated with each type of critical asset, assess the risks, and develop countermeasures to protect the critical assets.

4. Insider Threat Response plan

   In the SANS report titled "Insider Threats and the Need for Fast and Directed Response", SANS describes a survey conducted across 772 respondents which finds that 65% of organizations do not have adequate response plans in place for insider threat incidents.



Source: SANS (2015)

An insider threat response plan is different than a response plan under CIP-008 Incident Reporting and Response Planning standard requirements. Insider threat response plans should also cover financial and business impacts and multidepartment response actions, predominantly involving HR, Legal and law enforcement to detect, deter and respond adequately to reduce damage. The Center for Development of Security Excellence (CDSE) "Insider Threat Mitigation Responses" report is a useful resource for developing an adequate insider threat response plan.

5. Insider Threat Program Governance

Effective implementation of an Insider Threat Program requires effective governance. Entities can identify system and user activities to monitor, based on the risks to critical assets identified. Effective governance also includes the plan for communication and handling of insider threat events. An Insider Threat Program communication plan should at a minimum consider: (1) what types of events should be communicated; (2) whom to notify and when, (3) escalation mechanisms, and (4) notification timeframes for timely responses. Carnegie Mellon University's Common Sense Guide to Insider Threats provides additional information about Insider Threat Program communication plans.

6. Enterprise Risk Management Integration

To maximize effectiveness and awareness, entities should consider integrating their Insider Threat Programs into their overall enterprise or security risk management programs.

In future newsletters, I will discuss other key components of Insider Threat Program implementation. Please feel free to email me with questions or to share your thoughts on how you have implemented an Insider Threat Program in your organization.

References:

https://www.veriato.com/docs/default-source/collateral-assets/insider-threat-maturity-report.pdf

https://fas.org/sgp/obama/insider.pdf

https://www.dni.gov/files/NCSC/documents/nittf/20181024_NITTF_MaturityFramework_web.pdf

https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=34017

https://www.dni.gov/files/NCSC/documents/nittf/National_Insider_Threat_Policy.pdf

https://www.sans.org/reading-room/whitepapers/threats/paper/37447

https://www.cdse.edu/documents/student-guides/insider-threat-mitigation-response-options.pdf

Lessons Learned

By: Tony Purgar, Manager Event Analysis & Situational Awareness

The ERO Enterprise publishes lessons learned to provide entities with technical and understandable information that assists them with maintaining the reliability of the bulk power system. RF's EASA Team works with NERC and our entities to create and share Lessons Learned from both our region and other regions. Lessons Learned can be found on NERC's homepage (NERC.com) under the Reliability Risk Management program area.

The following Lessons Learned documents were newly released on February 28, 2019:

Current Drone Usage

- This Lessons Learned document is the result of a collaborative ERO EA effort with the primary interest group being Transmission Owners, Transmission Operators, Generator Owners, and Generator Operators .

- Some entities have begun using unmanned aerial vehicles (UAVs), commonly called "drones," for various purposes, such as major storm damage survey, line repair, substation/switching station and line inspections, power plant inspections, gas pipeline inspections, and security. Many transmission tasks currently done with helicopters can be completed by or supplemented with drones, resulting in reduced cost, increased safety, and more schedule flexibility. Additional uses and benefits are likely to develop through utilizing this emerging technology.

- The document highlights Reliability and Resilience Benefits including:
    - Storm damage recovery
    - Line, Structure, and Substation Inspections
    - Station Security
    - Generation Inspection
    - Lessons Learned:
        - Decision Makers Need to be Informed of Costs/Benefits
        - Rules one entity set for itself regarding drones
        - Using drones for patrolling lines
        - Understand Drone Limitations
        - Recovery on loss of guidance signal
        - FAA Regulatory Requirements must be addressed

Continued on page 6

Lessons Learned

Continued from page 5

Substation Fires: Working with First Responders

- This Lessons Learned document comes from WECC with the primary interest group being Transmission Owners, Generator Owners, and Distribution Providers.

- The document details two substation fire events that highlight the importance of having an incident response procedure and command structure, including Corrective Actions for each event.

- Lessons Learned (from both events)
    - Before a substation fire occurs, establish a working relationship with local fire departments. Discuss the hazards present in substations and exchange information on how to address substation fires. This document can be a starting point for that conversation.
    - Ensure the protocol for assuming the incident commander role is documented and understood by personnel:
        - Emergency Notifications
        - Incident Command
        - Predetermine an Access Plan
    - Forced Entry/Company Escort
    - Incident Size-Up
    - Transformer fire contingencies
    - Command Center
    - Transformer and other oil fires
    - Metal Switchgear
- Advice from an expert trainer to first responders
    - Transformer fire suppression is a two-step process
    - Switching
    - Leakage to the Nozzle
    - Pattern
    - Pressure
    - Product: Water, NFPA Agenda, Dry-Chemical, Drafting
    - Safe Standoff Distance
    - Electrical Test Standard: NFPA 18a – chapter 8, Section 8.5.
- Fire Service Response Posture
    - Entity and fire Department Preplanning
    - Response
- The document includes definitions and links to useful information regarding:
    - FEMA's National Incident Management System (NIMS) defining the Incident Command System (ICS)
    - "The Hat" – Identifying the Point of Contact / Incident Commander
    - Alleviating Forced Entry
    - Polychlorinated biphenyls (PCBs)
    - Preparedness Drawings & Photos
    - Temporary Station Power
    - A Foam Initiative / Better than Foam?
    - The International Associate of Fire Chiefs (IAFC)
    - The National Volunteer Fire Council (NVFC)

By: Midcontinent Indpendent System Operator, Inc.

Changing Resource Mix Results in Stakeholder Collaboration and MISO Tariff Changes

MISO's Resource Availability and Need (RAN) effort is designed to ensure that resources committed to serve MISO customers are available to provide sufficient energy and flexibility to serve that load throughout the year. A combination of factors in the MISO region have resulted in a resource portfolio with changing operating and availability characteristics. These trends are further complicated by reduced reserve margins, increased forced outage rates, and changing market conditions.

For example, some resources within MISO (such as Load-Modifying Resources or LMRs), may only be accessed through set emergency operating procedures, such as Maximum Generation Alerts or Events.

In the past, these emergencies occurred every year or two during extreme operating conditions. More recently, there have been 19 Maximum Generation Alerts since the start of the 2016/17 Planning Year, occurring mostly outside peak load periods. Some of these alerts progressed to become warnings or events. This is an evolution from historic patterns where resource sufficiency was only a risk in the peak load periods of summer and winter.

Are Generation Alerts the New Normal?

This recent increase in Maximum Generation declarations is symptomatic of interrelated long-term trends, including: an aging fleet, correlated generator outage planning practices, and growth of new resource types such as wind and demand response.

These trends impact the efficient conversion of committed capacity to energy, driving increasingly notable challenges to MISO's ability to serve load reliably throughout the year.

Informed by long-term trends, MISO's RAN program is focused on four goals:

1. Improving Outage Scheduling and Expectations;
2. Linking Resource Accreditation and Requirements with initial focus on Load-Modifying Resources (LMRs);
3. Aligning Planning Resource Auction (PRA) Commitments with Energy Needs all year; and
4. Ensuring Flexible Resource Availability to Address Changing Fleet Characteristics.

Stakeholder Collaboration and Resource Availability

RAN discussions were rooted in issues shared with MISO's stakeholders as early as 2015 and gained momentum in 2017 and 2018 with assignment through the MISO stakeholder process. Subsequent discussions have focused on understanding the challenges faced in converting committed capacity to energy.

These discussions first informed detailed issues whitepapers [found here] that further explored each of the trends, and then guided a potential solutions whitepaper [found here] that laid out a range of improvements to address the identified issues for now and the future.

A workshop in late 2018 further refined issues for near-term action. Potential changes are being considered in light of the established roles and responsibilities of MISO and its stakeholders, recognizing that resource adequacy, which ensures sufficient generation is installed to meet peak load-serving needs, is the obligation of states and Load Serving Entities (LSEs) and that generator outage scheduling is primarily the responsibility of resource owners. MISO's primary role remains focused on planning and operating a reliable and efficient transmission system to maintain reliability.

MISO has put forward a multi-phased action plan that pairs near-term improvements with longer-term holistic solutions to provide a sustainable framework for the future. Near-term efforts include performance improvements to LMRs and the planned outage process. The initial goal of implementing short-term fixes in early 2019 is tied to ensuring continued reliability starting in the spring 2019 outage season, historically a time when generator outage requests increase, while allowing full consideration of longer-term holistic solutions. Tariff filings were made with the Federal Energy Regulatory Commission (FERC) in December 2018 and January 2019 to address these matters (*see* FERC Docket Nos. ER19-650, 651 and 915). FERC approved the first such filing, which addresses LMR accreditation, in February 2019.

Continued refinements and longer-term holistic solutions are targeted for implementation in 2020 and 2021. These solutions are expected to include continued refinements for the 2020 Planning Resource Auction followed by movement toward holistic market-based solution(s). MISO and its stakeholders continue to face head-on the changing and challenging resource mix for a more efficient and more reliable bulk electric system now and in the future.

The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

CIP Supply Chain Cyber Security Requirements in Depth (Part 1 of 2)

Big Sable Point, MI - Photo by Lew Folkerth

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 November/December 2018 article, I discussed CIP-013-1 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 January/February 2019 article I provided a suggested structure for a risk management plan. In this article I'll dive into supply chain risk management Requirements for CIP-013-1 in more detail. I'll cover CIP-005-6 and CIP-010-3 in the next issue. Please remember that what follows are my opinions and my suggestions.

If you choose to adopt any of these suggestions, you must adapt them to your entity's position in the Bulk Electric System, and to your entity's systems and policies.

In the discussion that follows, I will quote only short phrases from the Standards. Please follow along in the actual Standards, available on the NERC web site here. In most cases I will paraphrase the Standards as I understand them. As always, the language of the Standard will govern in any compliance monitoring engagement.

CIP-013-1 Overview

CIP-013-1 is a forward-looking Standard that requires you to modify the way you work with your vendors in any future system, software, or service acquisition. You will have fulfilled the security objectives of CIP-013-1:

- if you integrate vendor and product security considerations into your vendor selection process,
- if your future acquisition contracts work to mitigate the cyber security risks posed by your selected vendor, and
- if you manage the relationship with each of your vendors, present and future, to mitigate risks you identify as applicable to the vendor.

CIP-013-1 applies to your high and medium impact BES Cyber Systems only. I recommend that you also include EACMS associated with high and medium impact BES Cyber Systems, as CIP-013-2 is expected to include these systems in its scope.

CIP-013-1 R1

You are required to develop and document at least one risk management plan. This plan must address the cyber security of your supply chain by implementing processes used in planning for procurement and in procuring systems. I discussed a possible structure for such a risk management plan in my January/February 2019 column. You may choose to create more than one plan for this purpose – for example, you might want to have separate plans for your control centers, transmission substations, and generating plants. Each plan must include the three types of processes specified by Parts 1.1 and 1.2, as discussed below.

Since these processes are part of a risk management plan, you will need to identify the risks applicable to your acquisition, assess those risks, select the risks you will address, and implement, in your purchasing process, remediation for those selected risks. The Standard is silent on exactly which risks you must address, which means you will need to develop this list on your own.

I recommend that your risk management plan include an assessment of the risks listed below, "Cyber Security Supply Chain Risk Consideration: A Starting Point." I intend this list to be used to spark your thinking and for you to build on as you identify additional risks. You should add risk identifications of your own to this list.

Continued on page 9

Continued from page 8

Addressing your identified risks will probably include some additions to the terms of any contract you use for acquiring BES Cyber Systems and systems or services related to BES Cyber Systems.

Two possible sources for acquisition contract language are:

- "Cyber Security Procurement Language for Control Systems," available here; and
- "Cybersecurity Procurement Language for Energy Delivery Systems," available here

The procurement language can be used as a source for possible risks, and for language to address selected risks in contracts. You will need to supplement your selected items with language to address threats that have emerged since these documents were published. For example, you may wish to ensure your vendor complies with US CERT's "SMB Security Best Practices" (here) in order to reduce the risk of ransomware within your ESPs.

Be careful when determining the scope of the risks you are considering. You can easily be distracted by valid risks that are outside the scope of CIP-013-1. CIP-013-1 only requires you to consider risks that can be addressed in planning and procuring systems and services related to BES Cyber Systems. Examples of risks that are outside the scope of CIP-013-1 might include an employee plugging in an unauthorized flash drive, or the risk of a poorly configured relay causing damage to BES components. These are both valid risks, and you should consider them elsewhere in your risk management plans, but they are not related to your supply chain and therefore are not in scope for CIP-013-1.

The processes specified by Parts 1.1 and 1.2 deal with vendor interaction, either in planning for procurement or in the actual procurement of systems. The term "vendor" is unofficially defined (see sidebar) in CIP-013-1. I say unofficially because the definition is not included in the NERC Glossary and is not part of the enforceable language approved by a regulatory authority. While I don't anticipate issues with the supplied definition, I recommend caution in relying on it.

Definition of *vendor*

"The term vendor(s) as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A vendor, as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators."

--- CIP-013-1 Guidelines and Technical Basis

Part 1.1 – Planning for Procuring and Installing

Your supply chain cyber security risk management plan must include a process that will be "used in planning for the procurement" of high and medium impact BES Cyber Systems. The process must address the identification and assessment of cyber security risks to the BES from vendor products or services. The cyber security risks addressed by this process would result from procuring and installing vendor equipment and software, or using services provided by the vendor. In other words, you must have a process that specifies how you will plan future acquisitions of products or services that will become, or will affect, BES Cyber Systems.

Part 1.1 – Planning for Transitions

In addition to the risks resulting from procuring and installing vendor equipment and software, Part 1.1 also requires your supply chain cyber security risk management plan to include a process that addresses cyber security risks resulting from transitions from one vendor to another. In other words, you must have a process that specifies how you will plan your future acquisitions of products or services such that the risks resulting from a vendor transition are minimized.

Part 1.2 – Procuring BES Cyber Systems

Your supply chain cyber security risk management plan must also include a process for procurement of BES Cyber Systems. Note that Part 1.1 requires processes to be used in *planning* for procurement and transitions; Part 1.2 requires a process to be used in actually procuring systems. These will probably be different but related processes.

Part 1.2 contains six sub-parts that specify items you must address in the procurement process. You should also include the additional procurement considerations identified by your Part 1.1 risk assessment.

In this article, I listed the required processes as separate processes, but there is no reason you can't combine processes to suit your needs. Just be sure you can clearly show an audit team that you address all required process types in your supply chain cyber security risk management plan.

CIP-013-1 R2

Any purchase arrangement or contract you enter into on or after the CIP-013-1 effective date of July 1, 2020, must be developed in accordance with your approved supply chain cyber security risk management plan.

For Requirement R2 you must implement all the supply chain cyber security risk management plans developed under R1. Any shortcoming in implementing your processes, and what they say you will do, could be considered a violation. This is different from a prescriptive Standard. For example,

Continued on page 10

Continued from page 9

if your personnel risk assessment process created by CIP-004-6 Requirement R3 says that you will perform personnel risk assessments every five years, but you miss that target by a year for some personnel, then that should not be a violation as you are still within the timeframe prescribed by the Standard. CIP-013-1 is different in that it is a non-prescriptive, risk-based Standard. You set the compliance rules in R1 by creating the plan and processes you will follow. You are then expected to follow through by implementing these self-generated requirements in R2.

Both contract language and vendor performance to a contract are explicitly taken out of scope for these Requirements by the Note to Requirement R2. I recommend that you do not rely on contract language to demonstrate your implementation of this Requirement. Instead, I suggest the implementation of your processes include documentation that you have followed these processes step-by-step.

This is in line with my recommendations in other articles that you always document your work so you can verify and validate that your processes are executed. For example, the effectiveness of your process for vendor incident notifications might be demonstrated by documenting actual or simulated notifications from the vendor, including your response to such notifications.

CIP-013-1 R3

You are required to obtain CIP Senior Manager (or designated delegate) approval for the supply chain cyber security risk management plan on or before the initial enforcement date of July 1, 2020.

To ensure that your supply chain cyber security risk management plan remains up-to-date, you are required to review it at least every "CIP year," or 15 calendar months. I strongly recommend that you consider reviewing the plan on either a shorter timeframe or have a provision to review the plan based on need (such as an emerging threat or a pending major procurement).

Each review should take into account any additional risks that have emerged since the prior review and should require those newly-identified risks to be added to your existing risks.

The entire assessment and remediation cycle should be performed to include consideration of the new risks. Each review should be documented and each time the plan is revised it should be approved by the CIP Senior Manager (or delegate).

Cyber Security Supply Chain Risk Consideration: A Starting Point

1. Obsolescence of the underlying platform

The expected lifetime of a SCADA, DMS, or other type of control system frequently far exceeds the expected lifetime of its underlying commercial hardware and operating system. How will you manage the risk of your hardware or software becoming unsupported? Will your vendor support a migration to an updated platform at a reasonable cost?

2. State of the art security

Will your vendor enable use of state-of-the-art security enhancements such as application whitelisting or software defined networking? Is the vendor flexible enough to adapt to newer techniques as they emerge?

3. Virtualization

If your vendor supports, or even requires, use of virtual systems, does the vendor support them in ways that are compatible with the currently enforceable CIP Requirements? For example, if the vendor mixes traffic from trusted networks (such as Electronic Security Perimeters) and untrusted networks on the same network hardware, this may put you at risk of a compliance finding.

4. Purchasing counterfeit hardware or software

How will you know that all components of the system you are acquiring are those actually made or approved by the system vendor? This is not usually an issue when a trusted vendor supplies all the components. But if you plan to purchase some components from another source, how will you mitigate the risk of obtaining compromised or substandard equipment?

5. Installing compromised genuine hardware or software

In 2017, the Danish shipping company Maersk installed one copy of compromised software on an internal computer. This software was provided by the original developer, but that developer had been compromised and malicious code placed in an updated package. This resulted in the compromise of nearly every computer within the company and paralyzed its global operations for an extended period of time.

6. Vendor personnel

If vendor personnel are to be granted access to your systems for any reason,

Continued on page 11

Continued from page 10

how will the vendor demonstrate to you that those personnel have been appropriately screened and trained? What controls will the vendor agree to for this purpose?

7. Vendor VPN access

If vendor personnel are to be permitted remote access to your systems via VPN, how will the vendor manage the risk of compromising your systems due to weak security at the originating computer? If the originating computer has been compromised, the malware will have access to your Intermediate Systems and will put them at risk. Similarly, if the originating computer is permitted to talk to both your systems and to other networks (such as the Internet) at the same time, your systems may be exposed to traffic from unexpected sources. This is known as “split tunneling.”

8. Vendor system-to-system access

If systems at the vendor’s location are permitted direct access to your systems, any compromise or weakness in the vendor’s systems will put your systems at risk. How will the vendor manage this risk? How will you know that the vendor is managing this risk?

9. Vendor information management

If your vendor will retain sensitive information about your systems such as, for example, network diagrams or administrative account credentials, how will the vendor protect this information? Will you be notified if this information is compromised?

10. Vendor internal security precautions

If your vendor is providing a service to you, such as a managed security service provider that performs log analysis and alerting, how does the vendor protect its own internal systems? Will you be able to assess the effectiveness of the vendor’s protections? Will you be notified of any compromise of the vendor’s systems?

11. Vendor termination process

When you discontinue your relationship with a vendor, will this transition proceed in an orderly, defined manner? What happens to any sensitive information in the vendor’s possession?

12. Adaptability to new risks

When ransomware appeared as a threat in early 2018, many entities were forced to make rapid changes to their network environments. Will your vendor support rapid response to emerging threats?

13. Vendor acquisition or dissolution

If your vendor goes out of business or is acquired by a different company, how will you support your system? Will you have access to the source code? Will licenses expire?

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.

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.

Regulatory Affairs

U.S. Senate Energy and Natural Resources Committee Holds Hearing to Examine the Electricity Sector in a Changing Climate

Discussions surrounding climate change, or the interchangeably used description “global warming”, has often proved to be an inherently political exchange. However, on March 5, 2019, during a hearing of the Senate Committee on Energy and Natural Resources, Republican Senator Lisa Murkowski, the Chair of the Committee, and Democratic Senator Joe Manchin, the ranking Democrat, both noted that from an energy and natural resources perspective, climate change is impacting citizens’ daily lives.

From this overarching agreement comes changing priorities and new areas of policy consideration which were reflected by the diversity of solutions discussed during the hearing, including micro-grids, carbon capture policy and grid efficiency.

Yet, the Committee remained cognizant of the reality that climate change and carbon emissions are just a portion of their responsibilities, and affordability and grid reliability remain key priorities. Senator Murkowski emphasized finding “pragmatic contributions” and developing “reasonable policies” to address the complexity of the issues facing the Committee.

Murkowski’s counterpart, Senator Manchin, emphasized noticeably similar inclinations towards pragmatism, highlighting the need for solutions which are “grounded in reality”. Following the hearing, Senators Murkowski and Manchin jointly published an op-ed discussing climate issues and the work of the Committee.

District of Columbia Clears Final Legal Hurdle for Power Line Undergrounding

On March 7, 2019, The District of Columbia Court of Appeals affirmed the rulings of the Public Service Commission of the District of Columbia (Commission) approving the first phase of the District of Columbia Power Line Undergrounding (DC PLUG) initiative.

DC PLUG is a joint effort between the Potomac Electric Power Company (Pepco), the District of Columbia Department of Transportation (DDOT), and additional agencies within the District to improve the electric service reliability and reduce the impact of storm-related outages by placing select systems underground.

In the spring, Pepco and DDOT are set to begin construction in the American University Park and Friendship Heights communities.

North American Generator Forum (NAGF) Update

By: Mike Gabriel, Deputy Chief Operating Officer, NAGF

NAGF – NPCC DER Collaboration

The North American Generator Forum (NAGF) and Northeast Power Coordinating Council (NPCC) Regional Entity are working collaboratively on emerging reliability issues related to grid edge DER. As these grid edge resources become more prolific, they will affect the Reliable Operation of the BPS.

The purpose of this collaboration is to raise awareness, identify benefits, provide outreach, and promote appropriate solutions for grid edge DER issues. Addressing these issues proactively with industry guidance and solutions rather than through mandatory and enforceable Reliability Standards will be beneficial to reliability, cost effectiveness, and operational/grid efficiencies.

NAGF and the NERC Modeling Task Force

During 2017, the NAGF sent a letter to NERC outlining various concerns with MOD-032-1. To address these issues, NERC's Power Plant Model Verification Task Force is developing a Reliability Guideline to address these concerns.

The goal of this Guideline is to promote consistency and uniformity in data requirements and reporting procedures, to the extent possible, between Planning Coordinators (PCs) and Transmission Planners (TPs) and Generator Owners (GOs). It is expected that this Reliability Guideline for MOD-032 Data Requests for Generating Resources will be published in 2019.

Upcoming NAGF meetings:

- Low Impact CIP Procedure Sharing (bi-weekly)
- Standards Review Team (monthly)
- AVR, PRC-005 and Protection System clarification - drafting meeting (weekly)
- NAGF ICE experiences webinar (April 23rd, 2:30-3:30 EDT)
- NAGF Annual Meeting & Compliance Conference: NERC's ATL Offices (October 15th-17th)

Standards Update

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

General NERC Standards News

Reliability Guideline Retired

The NERC Operating Committee approved the retirement of Reliability Guideline: Loss of Real-Time Reliability Tools Capability/Loss of Equipment Significantly Affecting ICCP Data. The rationale for this retirement is based on the fact that the general processes in the guideline have been covered in subsequent documents, including the Compliance Implementation Guideline on TOP-001-3 R13 and IRO-008-2 R4 Real Time Assessments. The full rationale can be found here.

Submittal Process Change for Standards Inquiries

Going forward, all Standards-related inquiries, such as Standard Authorization Requests (SAR) and Requests for Interpretation (RFI), should be submitted through the NERC Help Desk.

Lessons Learned Posted

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

- Current Drone Usage
- Substation Fires: Working with First Responders

Implementation Guidance Posted

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

- CIP-004-6 Personnel & Training, R4 and R5: Access Control for BES Cyber System Information (BCSI) Repositories Managed by Service Providers.

Other Resources Posted

NERC has posted the following resources:

- The streaming webinar and slide presentation for the PER-003-2 Requirement Training webinar. PER-003-2 – Operating Personnel Credentials will become effective on July 1, 2019.
- The streaming webinar and slide presentation for Project 2015-09 Establish and Communicate System Operating Limits (SOL). One topic discussed involved a concern regarding the logging and notification requirements for SOL exceedances.

Notable NERC Filings

In February, NERC filed the following:

- An informational filing regarding Reliability Standard TPL-007-3 – Transmission System Planned Performance for Geomagnetic Disturbance Events.

In March, NERC filed the following:

- A petition for approval of Proposed Reliability Standard CIP-008-6 – Cyber Security – Incident Reporting and Response Planning.

NERC's filings can be found here.

Notable FERC Issuances

In January, FERC issued the following:

- A letter order accepting NERC's compliance filing on amendment to the NERC Rules of Procedure to restore sections 603, 604, and 605, as well as correct typographical errors in sections 600 and 900.

In March, FERC issued the following:

- A letter order accepting NERC's filing of revisions to the Rules of Procedure, Appendix 4E – the Compliance and Certification Committee ("CCC") Hearing Procedures and Mediation Procedures; and,
- A delegated letter order approving NERC's filing of proposed amendments to Appendix 3A of the NERC Rules of Procedure – Standards Process Manual. The amendments will: (1) enhance processes for field test to support standards development for posting supporting technical documents; (2) improve the processes for appeals and interpretations; (3) provide language to clarify existing standard processes; and, (4) streamline language, address formatting items, and make other necessary changes.

FERC's issuances 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	Action	Start/End Date
Comment Period Open for Application Guide for Modeling Turbine-Governor and Active Power Frequency Controls in Stability Studies Draft Reliability Guideline	Submit comments via email using the comment form:	03/11/19 - 04/26/19

Recent and Upcoming Standards Enforcement Dates	
April 1, 2019	BAL-002-3- Disturbance Control Standard - Contingency Reserve for Recovery from a Balancing Contingency Event; EOP-004-4 – Event Reporting; EOP-005-3 – System Restoration from Blackstart Resources; EOP-006-3 – System Restoration Coordination; EOP-008-2 – Loss of Control Center Functionality
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)

These effective dates can be found here.

Networking Externally: NEO Operational Excellence Forum

ReliabilityFirst is a strong advocate of networking with other industries to share best practices and foster continuous improvement. On Thursday, April 18th, the Northeast Ohio Operational Excellence Forum held a “Gemba Visit” at ReliabilityFirst. A “Gemba Visit” is when people go right “to the work” to see how others perform best practices. ReliabilityFirst’s fifth floor conference room was full with operational excellence front-line practioners from these enterprises:

- The Federal Reserve Bank
- Akron Children’s Hospital
- Center for Dialysis Care
- Cleveland Clinic
- Defense Finance and Accounting Service
- Kavon International
- Caterpillar
- Rockwell Automation
- Honda
- Aspire Energy (Chesapeake Utilities)

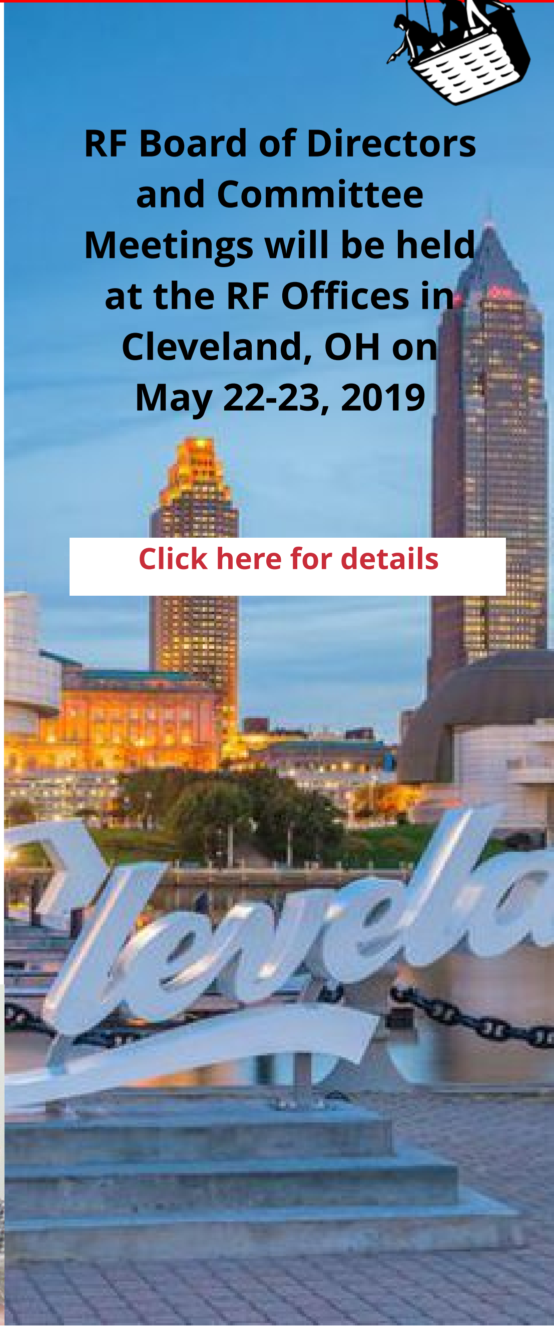
These diverse attendees generally practiced continuous improvement from multiple points of view depending upon their department/role. They often attend each other’s improvement events to stimulate new ideas. These were some of the various methods of continuous improvement represented:

- Change Management (HR)
- Lean Six Sigma (Operations)
- Agile/Scrum (IT and Software Development)
- Human Performance / Factors (Safety and Operations)
- Sustainability/Resiliency (HR)
- Diversity (HR)
- Innovation (Leadership)
- Project Management (Operations and Development)
- Systems Thinking / Design Thinking (Product/Service Development)

ReliabilityFirst CEO Tim Gallagher opened the meeting with an overview of the electric grid and the work of ReliabilityFirst. Dwayne Fewless, Senior Analyst, Events and Situational Awareness provided an interesting discussion of how ReliabilityFirst is uniquely designed to address the presidential challenges for lean regulation found in Executive Orders 12866 and 13563.

Participants broke into groups to discuss their continuous improvement experiences. The conversations focused on improving efficiency and effectiveness, while at the same time maintaining resiliency, sustainability, and corporate social responsibility. Here are a few ideas the teams came up with to help maintain this balance during continuous improvement activities:

- Capture the organization’s values when capturing requirements for a continuous improvement initiative
- Have “Control Plans” that address sustainability and resiliency
- Focus on team member strengths when possible during solution space discussions
- All of us have competition! Know them
- Keep the “why” goals in mind, not just the “how” and “what”
- Encourage innovation and measure it



RF Board of Directors and Committee Meetings will be held at the RF Offices in Cleveland, OH on May 22-23, 2019

Click here for details

2019 Innovation Awards and Retreat

In 2019, ReliabilityFirst hosted its second annual Innovation Awards and Retreat. The Innovation Awards and Retreat encourages innovators to try new ideas and projects, recognizes exceptional work in this area, and provides innovators access to individuals who can help them refine their innovations and make them happen.

A team of members from the ERO determined the criteria for judging submittals of innovations, and all ReliabilityFirst employees had an opportunity to make submittals. The award was presented during the Innovation Awards, which is a dinner and ceremony in honor of the winner and their team. During the ceremony, ReliabilityFirst executive leadership presents the Innovation Award, and guest speakers present on areas for potential future innovations. The Innovation Retreat (the day following the Innovation Awards) is a day set aside for all submitters to workshop their innovations. The leadership team is on hand to spend time brainstorming and advising attendees on ways to push their innovations forward. The guest speakers from the Innovation Awards also attend to provide expert assistance and advice.

In December of 2018, Bhesh Krishnappa (Principal Analyst) won the Innovation Award for the Cyber Resiliency Metrics Project, which he received at the 2019 Innovation Awards and Retreat. The Cyber Resiliency Metrics Project is an effort to better measure the resilience of industrial control system networks. Working with Old Dominion University, Bhesh helped to create a novel qualitative process and tool that can help entities assess their strength in industrial control system resilience.

The 2019 Innovation Awards Dinner was held at the Crowne Plaza next to the ReliabilityFirst offices the evening prior to the Retreat. As a special feature, an instructor visited the group before dinner to teach some meditation techniques aimed at improving creative thinking skills. Then, Bhesh provided an overview of his research.

The 2019 Innovation Retreat was held the following day at the Pro Football Hall of Fame in Canton. Four guest speakers attended: Don Racey (electrical industry economist), Dr. Katrina Kelly (electrical engineering professor from University of Pittsburgh), Dr. Jian Guowei (communications professor from Cleveland State University), and Dr. Gail Fairhurst (communications professor from University of Cincinnati.)

The speakers provided their insights regarding the future of the electric grid reliability and security and how to best understand the organizational cultures of power companies using modern discursive techniques.

The speakers were joined by Mark Lauby and the RF Management Team to participate in a full day innovation workshop. During the workshop, participants reviewed ongoing innovation work in small groups, and offered ideas for improvement. At the end of the event, each person reported out the many contributions made for each new project.

Calendar of Events

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

Date	RF Upcoming Events	Location
May 1-3	RF Spring Workshop	Baltimore, MD
May 22	RF Board of Directors Committee Meetings	Cleveland, OH
May 23	RF Board of Directors Meeting	Cleveland, OH

Industry Events:

Date	Industry Upcoming Events
April 30- May 2	FERC Environmental Review and Compliance for Natural Gas Facilities Seminar (New Orleans, Louisiana)
May 16	FERC Open Meeting
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

New Jersey Celebrates Leadership in Offshore Wind Sector

The New Jersey Board of Public Utilities (Board) released a report updating the progress of the state's offshore wind goals since Governor Murphy signed the 2018 Executive Order No. 8, which fully implemented the Offshore Wind Economic Development Act.

Over the last year, the Board has established an Interagency Agency Taskforce on Offshore Wind (IATF), launched New Jersey's Offshore Wind Strategic Plan, and solicited bids for 1,100 MW of offshore wind. Board staff is presently reviewing the applications for 1,100 MW of offshore wind and an award announcement is expected by the end of June.

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 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