Issue 4
2019 July-August

INSIDE THIS ISSUE

RELIABILITY FIRST

Note from the President

Dear Stakeholders,

We work with a lot of companies, and one of the challenges we see time and again is dealing with change and perhaps more importantly, sustaining important improvements made via intentional change. In this issue, MISO shares its thoughts on the topic of change, in an article on creating a program for sustainable change. I just visited with the leadership team at MISO, along with my colleagues Sara Patrick of MRO and Jason Blake of SERC, and we were all impressed at the improvements MISO is implementing.

I'd like to draw your attention to a different type of change, grid transformation, which is the theme of our upcoming reliability workshop. In many ways, our Region is at the epicenter of this transformation, with baseload generator retirements, the rise in natural gas generation, and our work with multiple Reliability Coordinators. I hope that many of you will join us for a multi-perspective discussion of this topic that enhances understanding and improves coordination and reliability across our Region.

Transformations, transitions, and their implications are critical, but I'd also like to emphasize the ongoing work we do to maintain security and reliability. We have some excellent speakers lined up to discuss cybersecurity and critical infrastructure in October at our workshop. We also are hosting several focused workshops in our offices this week on protection systems and human performance. In this newsletter, you will also see several articles on internal controls, supply chain, and insider threats. It should come as no surprise we are exploring these important topics slowly and steadily, issue after issue because they have become so important to the work you do.

I hope to see many of you at our upcoming events, and thank you for all the work you continue to perform day in and day out that keeps our lights on.

Forward Together,

Tim

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

Follow us on:

Insider Threats - Personnel & Training - Part 4

By: Bheshaj Krishnappa, Principal Analyst

In the previous articles on Insider Threats, we discussed setting up an Insider Threat Program and hiring relevant personnel for the program and training. In this article we will explore data collection and analysis under an Insider Threat Program. This section deals with building and maintaining insider threat analytic and response capabilities to collect, review, and analyze information, and respond as needed to insider threats.

The data collection and analysis aspect of an insider threat program is crucial for gathering data from multiple sources to detect potential or ongoing insider threat behaviors and actions. The data collected comes from variety of sources, including IT, HR, Legal, user activity monitoring, counterintelligence, and personal and physical security. It is a good idea to leverage the existing capabilities or data already available within your company when beginning this effort.

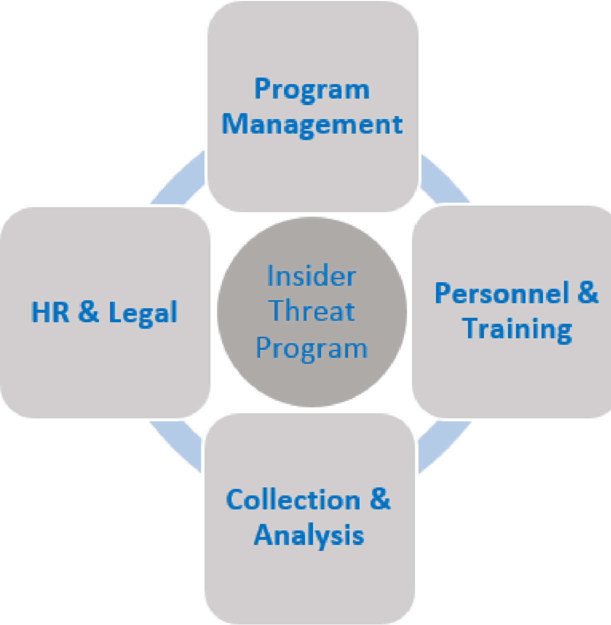
Some of the policies that need to be updated or referenced under data collection and analysis activities include:

- HR policies and procedures for monitoring employees or contractors,
- IT policies and procedures for user monitoring, information sharing
- Enterprise risk management policy
- Whistle blower policy
- Data collection and retention guidelines

The data collection and analysis function can be broadly classified under three sections: access to information, integrated data analytical capability, and prevention and response.

Access to information:

In order to identify, analyze, and assess the insider threat incidents, the designated insider threat personnel need to have access to data from multiple sources, such as host and network based logs, relevant HR indicators, and open source intelligence on cyber or physical security developments. The NERC CIP requirements under CIP-007-6 R4 – Security Event Monitoring involve cyber asset level monitoring more from an external threat perspective and can be leveraged for an Insider Threat Program as well. The CIP requirements mandate monitoring cyber assets that are directly responsible for BES operations. The following chart visually depicts the various technical and non-technical data sources that are relevant to institute a good program for managing insider threats.



Integrated data analytical capability:

The insider threat personnel are responsible for identifying insider threat risk indicators, responding to insider incidents, and creating or recommending controls to help prevent insider incidents. Insider threat personnel should analyze data from multiple sources, as seen in the diagram above, in a timely manner and respond to it. NIST Special Publication 800-92 provides guidance on developing, implementing, and maintaining effective log management practices throughout an enterprise, which is essential for an effective data collection and analysis capability. A good Security Information and Event Management (SIEM) tool can provide real-time analysis of security alerts generated by cyber or physical hardware and applications. Even though SIEM can be configured to alert on pre-defined patterns of malicious activity, sometimes a tool such as User Behavior Analytics tool can help personnel focus on the behavior of systems and the people using them in a timely manner.

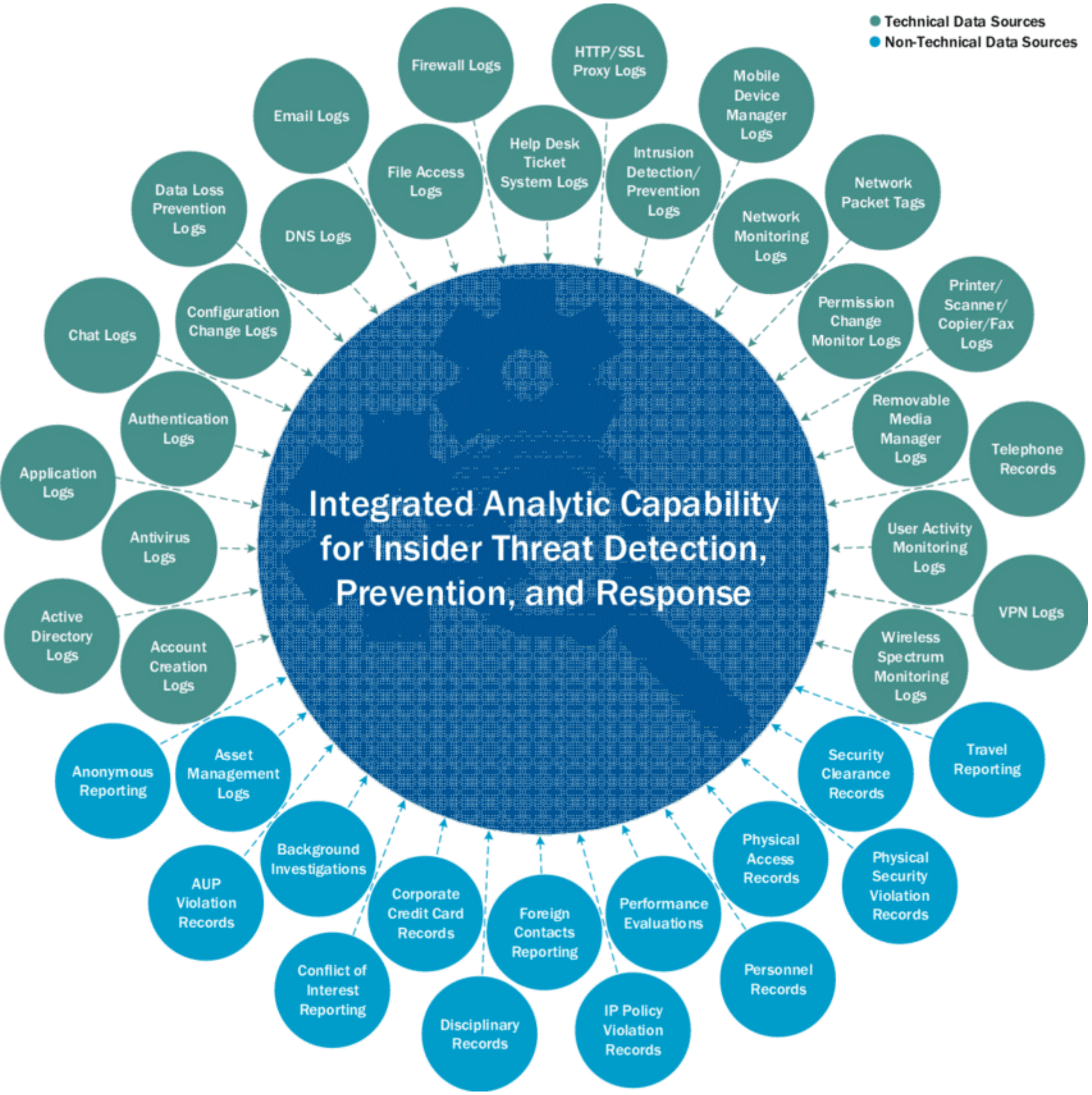
Prevention and response:

While analyzing insider threats it is important to ensure a fair assessment without infringing on employees' or contractors' civil liberties and privacy rights. According to the Center for the Development of Security Excellence (CDSE), the following questions should be considered:

Continued on page 3

Insider Threats - Personnel & Training - Part 4

Continued from page 2


● Technical Data Sources
● Non-Technical Data Sources
Integrated Analytic Capability for Insider Threat Detection, Prevention, and Response
Firewall Logs
HTTP/SSL Proxy Logs
Mobile Device Manager Logs
Email Logs
File Access Logs
Help Desk Ticket System Logs
Intrusion Detection/ Prevention Logs
Network Packet Tags
Data Loss Prevention Logs
DNS Logs
Network Monitoring Logs
Printer/ Scanner/ Copier/Fax Logs
Chat Logs
Configuration Change Logs
Permission Change Monitor Logs
Authentication Logs
Removable Media Manager Logs
Telephone Records
Application Logs
Antivirus Logs
User Activity Monitoring Logs
VPN Logs
Active Directory Logs
Account Creation Logs
Wireless Spectrum Monitoring Logs
Anonymous Reporting
Asset Management Logs
Security Clearance Records
Travel Reporting
Background Investigations
Physical Access Records
Physical Security Violation Records
AUP Violation Records
Corporate Credit Card Records
Foreign Contacts Reporting
Performance Evaluations
Personnel Records
Conflict of Interest Reporting
Disciplinary Records
IP Policy Violation Records

Source: Common Sense Guide to Mitigating Insider Threats, Fifth Edition (p.83)

- Is the individual currently harming the organization's resources?
- If so, is the harm intentional?
- Is there a risk that the individual will do so in the future?

As insider threats are a complex multi-faceted risk, the prevention and response requires a multi-faceted, multi-disciplinary approach. The CDSE has a course which helps entities to tailor their response options. The response options to curtail the effects of insider threats can vary by department. For example, the human resource department may employ counseling, training or termination. The cybersecurity group response may include downgrading system or user access privileges, increasing monitoring, or training to reinforce understanding.

Some insider threat events detected may call for modifications to existing procedures or policies. Hence, a periodic re-evaluation of data collection, analysis, prevention and response capability is required to learn from incidents and fine tune existing capabilities for a timely and effective response. Some incidents may require referral to local or national law enforcement agencies depending on the insider threat activity identified, and there should be policies in place to state when these referrals should take place.

In the next article we will discuss HR and legal aspects of insider threat management, including onboarding, investigations, policies and reporting.

References:

Computer Security Resource Center

Guide to Computer Security Log Management

Developing a Multidisciplinary Insider Threat Capability

Tripwire: When Deviations become Baselines

By: Tony Freeman, Senior Risk and Mitigation Analyst

In recent months we have heard a need for some clarity around software you may use to monitor your environment, specifically when a BES Cyber Asset change is officially a documented baseline within the Tripwire Application and at what time that occurs.

Once a change has been made to a system in which the Tripwire Agent has been installed, if configured correctly, Tripwire should alert on this baseline deviation, thus notifying the responsible entity that a change to the system(s) has occurred. It is assumed at this point that the responsible entity has ensured all other compliance obligations have been met, such as change management, security controls testing under CIP-010-2 R1.4 or if applicable R1.5.

When the baseline deviation is alerted upon by Tripwire it has been documented but it **has not** been verified against an approved change control ticket to ensure that the change was in fact authorized. At this stage this change **cannot** be considered part of the approved system(s) baseline(s) recorded documentation for high and medium impact BCS, EACMS, PACS, and PCAs under CIP-010-2 (Cyber Security – Configuration Change Management and Vulnerability Assessments) R1.

In this current state, prior to review, it would be considered an unauthorized change. However, it is a good internal control that provides documented evidence under CIP-010-2 R2, as monitoring for changes to baseline configurations every 35 calendar days, but does not provide the proper context and evidence for evidence into CIP-010-2 R1.2 and R1.3.

Considering these factors, the time of promotion would constitute that baseline deviation as an authorized change. This ensures that the entity has verified the detected deviation against an approved change control activity in order to determine that this change was in fact authorized. Also, this would be applicable to some of the Tripwire "auto-promote" functions such as "promote by change request.. This would ensure that an approved change request ticket can be matched to the deviation and said deviation is authorized to change baseline information thus recording the approved change and modifying the baseline as required.

Additionally, if you are not using the auto promote functionality you may want to consider a manual entry into Tripwire Profiler to show that a review of the change request versus the detected baseline deviation has occurred. By annotating the change request number inside of profiler, you can show the direct linkage to alert on the specified baseline deviation.

These recommendations can also be applied to a number of industry related products such as Industrial Defender, Splunk, or FireEye that aim at the same goals as Tripwire. Tying change information directly together with the application's alerts and/or logs for system changes will help you better document system(s) change(s) providing for higher quality evidence for internal reviews or audit preparations.

If you have any additional questions, comments, or concerns regarding Risk Analysis, Mitigations, or Evidence please feel free to contact the RF Risk Analysis and Mitigation (RAM) department here and select "Risk Analysis & Mitigation"

Get Control of Yourself!

By Denise Hunter, Principal Technical Auditor

Hello and welcome back! This month I am going to address a risk element that has been garnering more attention lately, specifically ***Gaps in Program Execution***. This risk element focuses on the emerging risk created by processes and controls not adequately implemented, or consistently applied. The 2019 Compliance Monitoring and Enforcement Program Implementation Plan identified FAC-003-4, FAC-008-3 and PRC-005-6 as the standards with highest number of incidents where inconsistent or inadequate controls are believed to be contributing to increasing the risk posed by the standard. In preparation for this article, I researched how prevalent that risk exposure was.

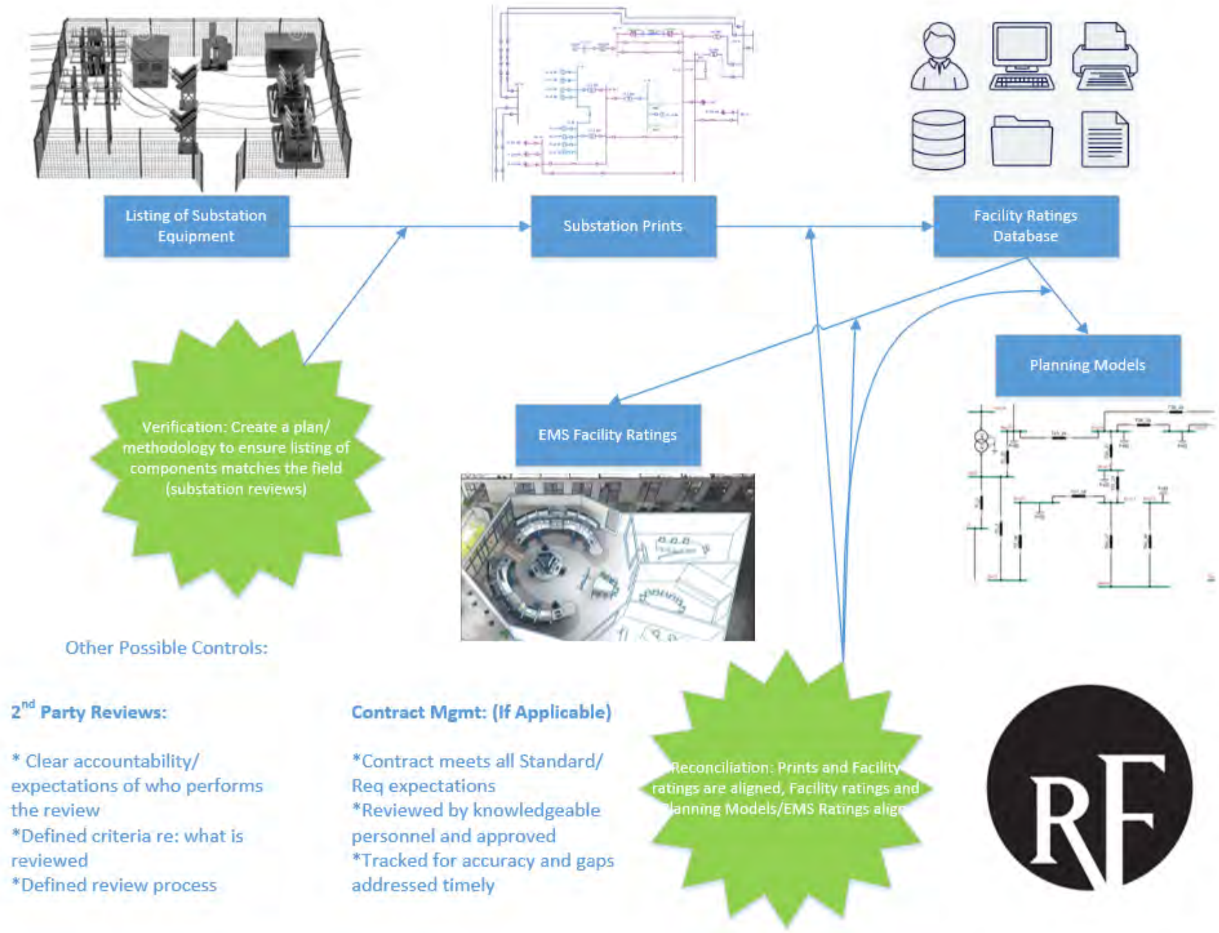
Over the course of the current version for those three standards, NERC has identified 24 Notice of Penalties across the ERO, with FAC-008-3 accounting for 19 of those violations. **Nineteen!** This warranted further research to identify what one control failure was the highest contributor to that figure. It turns out that it wasn't just one control, it was a number of controls that were failing. This increased the risk exposure, so I am going to veer from my previous method of focusing on one internal control, and I will speak to each control failure identified, and provide focused information on one.

Nine of the nineteen violations of FAC-008-3 were based on a failure of R6, " *Each Transmission Owner and Generator Owner shall have Facility Ratings for its solely and jointly owned Facilities that are consistent with the associated Facility Ratings methodology or documentation for determining its Facility Ratings*."

You might ask 'How is this possible? We have written a thorough methodology addressing all expected criteria, ensuring that we have properly identified the most limiting Element! What went wrong?' In answer to that question: you can write the most thorough methodology for any process, but without appropriate training, controls for the implementation process, and monitoring the performance of that methodology, the methodology will likely eventually fail.

So what controls were missing and why did they fail? Let's look at the details for a few of those events and see if we can answer that question. For each event, I will suggest a mitigating control that might have prevented the occurrence.

These five events on the following page represent the majority of the control failures reported. See the figure to the right for a visual representation, with possible additional controls:



Listing of Substation Equipment

Substation Prints

Facility Ratings Database

Planning Models

Verification: Create a plan/ methodology to ensure listing of components matches the field (substation reviews)

EMS Facility Ratings

Other Possible Controls:

2nd Party Reviews:

* Clear accountability/ expectations of who performs the review
*Defined criteria re: what is reviewed
*Defined review process

Contract Mgmt: (If Applicable)

*Contract meets all Standard/ Req expectations
*Reviewed by knowledgeable personnel and approved
*Tracked for accuracy and gaps addressed timely

Reconciliation: Prints and Facility ratings are aligned, Facility ratings and lanning Models/EMS Ratings alig

Continued on page 6

Get Control of Yourself!

Continued from page 5

Event 1

Entity discovered while performing a gap assessment after taking over facility operations from a previous owner that the entity facility ratings did not include all the required components specified in FAC-008-3 R6.

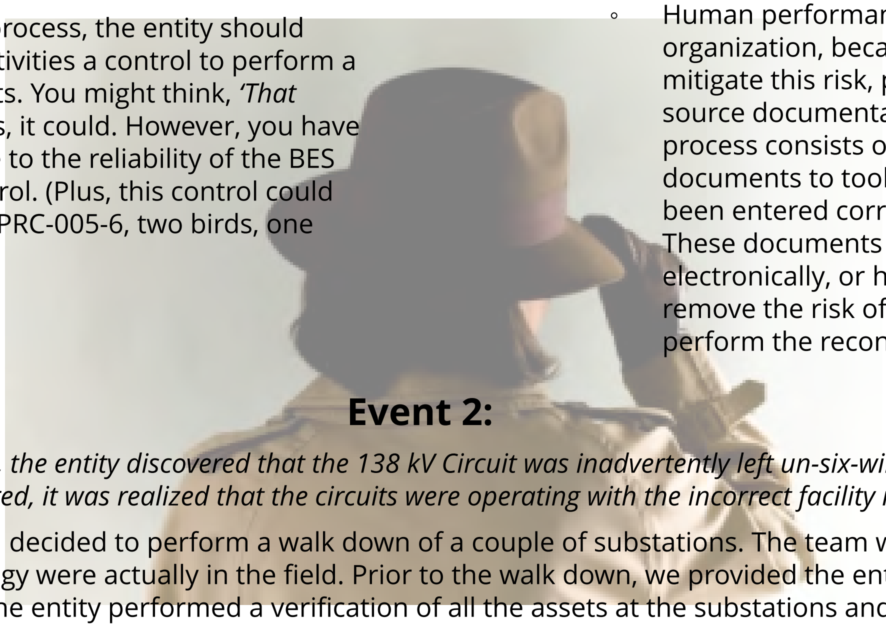
This is a common occurrence. An entity grows their business through a merger or acquisition, and by doing so assumes the risk that the previous owner did not adequately mitigate due to inadequate assessments or an unsound methodology.

- Mitigating control for Event 1: Verification of asset listing. (Detective Control)
    - During the acquisition/merger process, the entity should include in their due diligence activities a control to perform a complete verification of all assets. You might think, *'That could be a huge undertaking!'*. Yes, it could. However, you have no idea what your risk exposure to the reliability of the BES is, without performing that control. (Plus, this control could help mitigate any risk posed by PRC-005-6, two birds, one stone!!)

Event 3

An entity used the Substation Conductor Ratings Determination Tool. The tool uses user-based assumptions and equations from various standards to calculate parameters for the equations and the ambient temperature ratings for substation conductor types. The entity then discovered inconsistencies with the tool and certain substation conductor ratings, and determined the issues arose from a data input error. The resulting review required a change in ratings for 3% of the entity's BES transmission facilities, to mitigate the violation.

- Mitigating Control for Event 3: Reconciliation of data input. (Detective Control)
    - Human performance is the largest risk posed by every organization, because human beings are fallible. In order to mitigate this risk, perform a reconciliation of input data to source documentation to ensure accuracy. The reconciliation process consists of simply 'ticking and tying' the source documents to tool documents, ensuring that all data has been entered correctly, then signing and dating the report. These documents can then be scanned and saved electronically, or hardcopies maintained. If possible, to remove the risk of cognitive bias, a separate individual should perform the reconciliation.



Event 2:

During a combined training/station review session, the entity discovered that the 138 kV Circuit was inadvertently left un-six-wired for the first span on both circuits near the substation. Once the incorrect design was discovered, it was realized that the circuits were operating with the incorrect facility ratings documented.

I was recently on an audit where the audit team decided to perform a walk down of a couple of substations. The team was reviewing the Facility Ratings to compare what Elements used in the methodology were actually in the field. Prior to the walk down, we provided the entity a listing of possible substations under review. During their preparation for the audit, the entity performed a verification of all the assets at the substations and identified a number of facility rating issues. The entity was fully transparent and informed the audit team of their finding.

- Mitigating control for Event 2: Verification of asset listing. (Detective Control)
    - Incorrect asset listings due to component replacements, setting changes, human error, etc. occur, placing the reliability of the BES at risk. As stated above, I am aware that this could be a huge undertaking. However, the risk of not performing this control could place any other controls established around asset performance and asset maintenance in a suspect position. If your baselines were inadequate or incorrect, all other controls would be working off incorrect information. Establishing a schedule to perform this verification, in a systematic manner, that doesn't place your entity under undue stress, would go a long way to ensuring your reliability to the BES.

Continued on page 7

Get Control of Yourself!

Continued from page 6

Event 4

Entity had a concern about meeting system restoration requirements for a nearby nuclear plant. To address this concern long term, the entity was in the process of installing and testing a new Black Start Resource to supply the nuclear plant with power. But, because the modifications and tests were occurring around the same time as another substation's units (Substation A) were set to retire, the entity decided they would temporarily keep the Substation A's peaking units in its System Restoration Plan as backup Black Start Resources in case the modifications or tests were not successful or completed on time.

This decision keep the Substation A peaking units as backup Black Start Resources was not communicated to all necessary individuals. As a result, the individuals responsible for setting the Facility Rating for the Substation A peaking units incorrectly believed Substation A units were retiring in April 2016 and thus did not set a Facility Rating by the July 1, 2016 deadline.

- Mitigating Control for Event 4: Change Management (Preventative Control)
    - The greatest value of change management is that it provides conceptual scaffolding for people, the process, and the organization implementing change. It's a framework used to support and understand the change and its effect on the organization and its people.[1] We will discuss this control in more detail below.

Event 5

Engineering discovered that bus equipment ratings from Engineering correspondence used to identify the ratings did not match the vendor drawings for Gas Turbines at two different units.

As a result the bus ratings were incorrect for those two units. When the drawings were updated, these bus ratings became the Most Limiting Series Element (MLSE).

- Mitigating Control for Event 5: 2nd Party Review (Detective)
    - The strength of a review is that it removes the risk of cognitive bias, and provides a knowledgeable, objective assessment of the data or process, increasing the opportunity to identify inaccuracies.

[1] Benefits of Change Management

Continued on page 8

Get Control of Yourself!

Continued from page 7

Next, I would like to discuss the design of a strong Change Management control. The strength of a good Change Management control lies in the ability to ensure that all changes are approved and documented, services are not unnecessarily disrupted, and resources are used efficiently. It's a systematic approach to managing all changes made.

Here are some steps that I would consider when designing a Change Management control:

1. Entity has established a plan to identify when changes to operations or operating conditions, or deviations from established baselines, could negatively affect operation and therefore change is needed.
2. The entity has established a change approval process where changes are requested in a formal process, requests are recorded and assessed based on their projected effect to operations.
3. The entity has a developed a change implementation program that details proper coordination of approved changes to all internal and external stakeholders, in order to remove or reduce any interruption to operations.
4. Changes to operations are monitored in order to ensure that they are producing the desired outcome or effect.
5. Entity documentation of changes, whether in response to events or in accordance with plans or approved changes, follow the trail of the change from conception to monitoring, and capture all necessary information.
6. Entity has defined an emergency change process. Things can happen that require changes be made immediately. The entity should define a process to ensure they circle back and address the previous steps, to ensure the emergency change addressed all established criteria.

A strong Change Management control is imperative to help reduce the issues around FAC-008-3 implementation. Effective change management could ultimately help to reduce your misoperations rate by reducing the opportunity of error during relay replacement and maintenance work. A Win Win!!

Finally, I would like to talk about the monitoring process, because this is an extremely important process needed to ensure the accuracy, consistency and success of any control. The best controls are susceptible to failure if no one is monitoring the control. You create strong control environments by embracing all components of the internal control program (culture, risk assessment, control activities, information & communication, and MONITORING), however far too often the controls fail because no one was monitoring them consistently to ensure that they were still working effectively and efficiently.

New staffing, technology updates or changing organizational policies or structure will dilute a control and increase risk. Therefore, control monitoring is just as important as the design of the control.

Monitoring of controls is a cyclical process. It starts with:

1. an understanding of the control by people knowledgeable of the desired outcome
2. monitoring and evaluation of the control is performed on a consistent basis
3. if deficiencies are identified then the change management control is initiated resulting in a reevaluation or update to the control
4. if no deficiencies are identified, documentation of the monitoring is maintained

We've talked about a number of control activities today: Verification of Assets, Reconciliations, Change Management and the importance of monitoring controls. I hope that I haven't overloaded you with information, and the idea of identifying and including internal controls within your daily activities is beginning to be a little more familiar.

Until next time, enjoy the summer and Get Control of Yourself!

The Seam

Achieving Sustainable Change

The energy industry is undergoing profound and rapid change. The industry's ability to implement change effectively is an increasingly important strategic asset. Ideally, a potential reliability or security issue is identified and a systematic change is implemented to fix it before the issue turns into a problem. Change can be a challenge, however, because between 50 – 75% of organizational change initiatives fail. At MISO, we've used a variety of tools to achieve sustainable change, and the "levers of change," from the book Leading Successful Change by Greg Shea and Cassie Solomon, have been particularly effective.

Shea and Solomon contend that the majority of change initiatives fail for two reasons: (1) unclear objectives that don't focus on changing the behavior of people, and (2) failure to realize that unless you also change the environment people work in, they are likely to revert to the behaviors encouraged by the old environment.

To combat the first reason changes fail, Shea and Solomon suggest that you establish a scene or vision that focuses specifically on what you want people to achieve, like operating the grid reliably and securely. They also suggest that you identify the critical roles involved in transforming the scene you establish. Importantly, they encourage you to consider all levels of an organization, not just the most senior ranks. In MISO's case, that could be system operators, information technology professionals, and facilities support personnel. Shea and Solomon then encourage you to explain how all the roles work together from the perspective of each role to provide clarity about the behaviors you want to encourage.

Once you have established the desired behaviors you want to see, Shea and Solomon suggest you design the work environment to foster those behaviors using the eight levers of change, which are:

- Organization - This is about an organization chart or a governance structure.
- Workplace Design - This is largely how to use physical and virtual space.
- Task - This is processes and procedures.
- People - This is a focus on multiple factors like skills, competencies, and workforce training.
- Rewards - This is about creating mechanisms for positive and negative reinforcement.
- Measurement - This returns us to the maxim "you get what you measure."
- Information Distribution - This is who knows what, when, and how.
- Decision Allocation - This is who takes part in decision-making and what role they play.

Shea and Solomon point out that successful changes use at least four of the levers of change and anything fewer than four is wasted effort. You may also need to pull change levers harder than you initially thought. For example, distributing a report to a small group might change behavior, but a report may need to be distributed at a higher level in the organization to ensure the change occurs. You may also need to add more change levers for change to take hold.

MISO adapted to the industry's pace of change by making improvements to its compliance program to continue to provide reliable and secure service to our customers. We are committed to implementing lasting change and have used Shea and Solomon's change levers approach to do so. We pulled all levers with varying degrees of force and at different times. While we plan to review and adjust our approach as we go, several examples of our recent efforts are provided below.

We began by reinforcing the scene of how important the reliability and security of the grid are to MISO's mission and talking about the day-to-day behaviors required to deliver on this critical mission. We used the Organization lever to consolidate compliance activities performed throughout MISO into a centralized group called "Standards & Assurance" and organized it by the functions performed. We used the Task lever to standardize and improve our own processes based on risk, which will fuel the company's excellence mindset above and beyond compliance.

We also employed the Information Distribution lever with process changes to increase timeliness and usefulness of information distributed to the correct people. As we do this, we are emphasizing the importance of face-to-face communications instead of email. We used the Decision Allocation lever to ensure that our process changes result in engaging the right decision-makers, including senior executives, the Chief Compliance Officer, senior management, and other employees, at the appropriate points in our processes. According to Shea and Solomon, the Decision Allocation lever, when aligned with the Organization, Task, and Information Distribution levers, creates clarity in approach and increases the likelihood of successful change. The summary of Shea and Solomon's book outlines an effective, systematic approach to implement lasting change. Of course, in order to sustain the changes MISO made, we must review our results and adjust as needed. We invite you to try their model with your next reliability initiative and share your experience!

The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

CIP Supply Chain Cyber Security Requirements in Depth (Part 3 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 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 Jan/Feb 2019 article I provided a suggested structure for a risk management plan. This article completes my series on the in-depth study of the supply chain cyber security risk management Requirements that was begun in the Mar/Apr and May/Jun 2019 issues. I'll also answer some questions that have been presented to me and to the ERO Enterprise. 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.

CIP-010-3 R1 Part 1.6

In Order 829 at P 48-50, FERC required NERC to develop a Reliability Standard to address the verification of both the identity of the software publisher and the integrity of all software and patches for BES Cyber Systems. FERC stated that the objective of these changes is to reduce the likelihood of the installation of compromised software on a BES Cyber System.

In response to Order 829 P 48-50, one new part has been added to CIP-010-3. You are required to perform software verification by verifying the integrity of both the software source and the software itself. Here's the enforceable language of Part 1.6:

R2: Each Responsible Entity shall implement one or more documented process(es) that collectively include:

Port Sanilac, MI - Photo by Lew Folkerth

Applicable Systems	Requirements
High Impact BES Cyber Systems: and Medium Impact BES Cyber Systems Note: Implementation does not High Impact BES Cyber Systems; and require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	Part 1.6: Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source: 1.6.1. Verify the identity of the software source; and 1.6.2. Verify the integrity of the software obtained from the software source.

Continued on page 11

The Lighthouse

Continued from page 10

Supply Chain Questions

The ERO has begun receiving requests for guidance regarding the application of the supply chain Standards, especially CIP-013-1. Here are the questions I've seen so far, and my answers to them.

Q: How many levels (tiers) of vendors must an entity consider for CIP-013-1 Compliance?

A: The responsibility for determining how deep into the vendor supply chain to delve lies with you, the Responsible Entity, through your supply chain cyber security risk management plan.

CIP-013-1 is silent on how deep into the vendor supply chain you must go. My recommendation is that you should know as much about your equipment, software, and services as possible. I suggest that you document as much as you can about your BES Cyber Systems and their makeup, using your CIP-010 baselines and expanding on each baseline with as much detail as you can gather. From this information you can compose a list of hardware, software, and services that are used in your systems.

CORRECTION

In my Mar/Apr 2019 article I said, "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." This is incorrect. It should read, "Any procurement begun on or after the CIP-013-1 effective date of July 1, 2020, must be performed in accordance with your approved supply chain cyber security risk management plan."

You can then assess your hardware, software, and service list based on risk. For example, you would probably assess the cyber security risk of a server power supply as very low. You would probably assess the cyber security risk of a network-connected out-of-band server management device as high or severe.

You should then be able to create a list of vendors of your devices, software, and services, and prioritize that list based on the assessed risk of each component a vendor supplies.

Q: If I buy routers at Office Depot, does that constitute a "contract" or is that just a procurement?

A: Any equipment, software, or services whose acquisition is begun on or after July 1, 2020, that will become or will be directly related to a high or medium impact BES Cyber System must be acquired in accordance with your supply chain cyber security risk management plan. The plan must be used whether or not a contract is involved. The only place in the enforceable language of CIP-013-1 where the term "contract" appears is in the note to Requirement R2. Risks incurred by acquisitions from vendors such as Walmart (yes, they do carry business-grade Cisco products) or sellers of new and used equipment on eBay are some of the risks this Standard is intended to mitigate. In particular, there could be an elevated risk of compromised or counterfeit hardware from such sources.

Enforceable Elements of a Standard

From the NERC Standard Processes Manual Section 2.5, "The only mandatory and enforceable components of a Reliability Standard are the: (1) applicability, (2) Requirements, and the (3) effective dates. The additional components are included in the Reliability Standard for informational purposes and to provide guidance to Functional Entities concerning how compliance will be assessed by the Compliance Enforcement Authority."

In addition, Glossary terms and Implementation Plans may be separately approved as mandatory and enforceable.

The term "contract" also appears in the definition of "vendor" in the Rationale section of the Standard, but that definition does not appear in the enforceable elements of the Standard. The definition may be useful as guidance, but be cautious about relying on the exact wording. For example, the use of "contract" in the definition appears to restrict the application of CIP-013-1 to only those parties with which the Responsible Entity has a formal contract. This restriction is not supported by the enforceable elements of the Standard, which means you cannot rely on that aspect of the definition.

Q: Will a Responsible Entity be expected to perform and document initial cyber security risk assessments on all its existing vendors that provide their BES Cyber System products and services prior to the compliance effective date?

A: No, CIP-013-1 affects only new procurements. This answer is supported by the General Considerations section of the Implementation Plan:

"In implementing CIP-013-1, responsible entities are expected to use their Supply Chain Cyber Security Risk Management Plans in procurement processes (e.g., Request for Proposal, requests to entities negotiating on behalf of the responsible entity in the case of cooperative purchase agreements, master agreements that the responsible entity negotiates after the effective date, or

Continued on page 12

Continued from page 11

direct procurements covered under the responsible entity's plan) that begin on or after the effective date of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in a contract do not determine whether the procurement action is within scope of CIP-013-1."

In order to determine the begin date of a procurement, you must document that date in a manner suitable for use as audit evidence. Without such documentation, audit teams will use the earliest date that provides reasonable assurance of the beginning of the procurement process.

Q: If I procured hardware or software from a vendor prior to 7/1/2020, but installed that hardware or software after that date, must I perform a risk assessment of that vendor?

A: Risk assessments of vendors that provided equipment, software, or services prior to the CIP-013-1 effective date of July 1, 2020, are not required. Any procurements for high or medium impact BES Cyber Systems equipment, software, or services begun after July 1, 2020, must be performed in accordance with your documented CIP-013-1 R1 supply chain cyber security risk management plan. Any software installed on or after July 1, 2020, must have its identity and integrity verified, regardless of when the software was obtained.

Q: Contracts for procurement that are in place prior to July 1, 2020, are not in scope for CIP-013. What about contract renewals?

A: CIP-013-1 applies to any procurements begun after July 1, 2020, regardless of the existence of a standing contract, and regardless of any revisions to such a contract. You are not required to invalidate or renegotiate any contract, but you must demonstrate that any procurement begun after July 1, 2020, has been performed in accordance with your supply chain cyber security risk management plan. You will need to establish a beginning date for the procurement. The effective date of a contract is not necessarily the beginning of a procurement. The beginning date might be the date of an expenditure authorization or a request for bid, quote, etc. You will then need to show how you followed your risk management plan throughout the acquisition.

Q: My source for equipment says that they are not a "vendor," but rather a "supplier," and so they are not subject to CIP-013-1. How do I answer this?

A: Any organization or person that supplies equipment, software, or services to your entity must be considered a "vendor" in the meaning of CIP-013-1. Your "supplier" is quite correct to say that they are not subject to CIP-013. Only NERC Registered Entities that are procuring hardware, software, or services that will become or that will directly affect high or medium impact BES Cyber Systems are subject to CIP-013-1. It is your relationship with each vendor, supplier, etc. that is subject to CIP-013-1, not the vendor itself. In managing that relationship you may use many tools, including purchase or acquisition contracts, existing vendor practices such as incident notification, existing or emerging security practices, such as software verification, vendor web site features such as digital certificates and digital signatures, and so forth. Although you may choose to manage your vendors through contracts, CIP-013-1 does not explicitly require this. If your vendor will provide a feature or a service as part of its ongoing security practices, there may be no requirement for a contract for such matters. And you may show that the implementation of your risk management plan accomplishes its goal of reducing supply chain risk by means other than contracts.

Requests for Assistance

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

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

Feedback

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

I may be reached here.

In the Industry

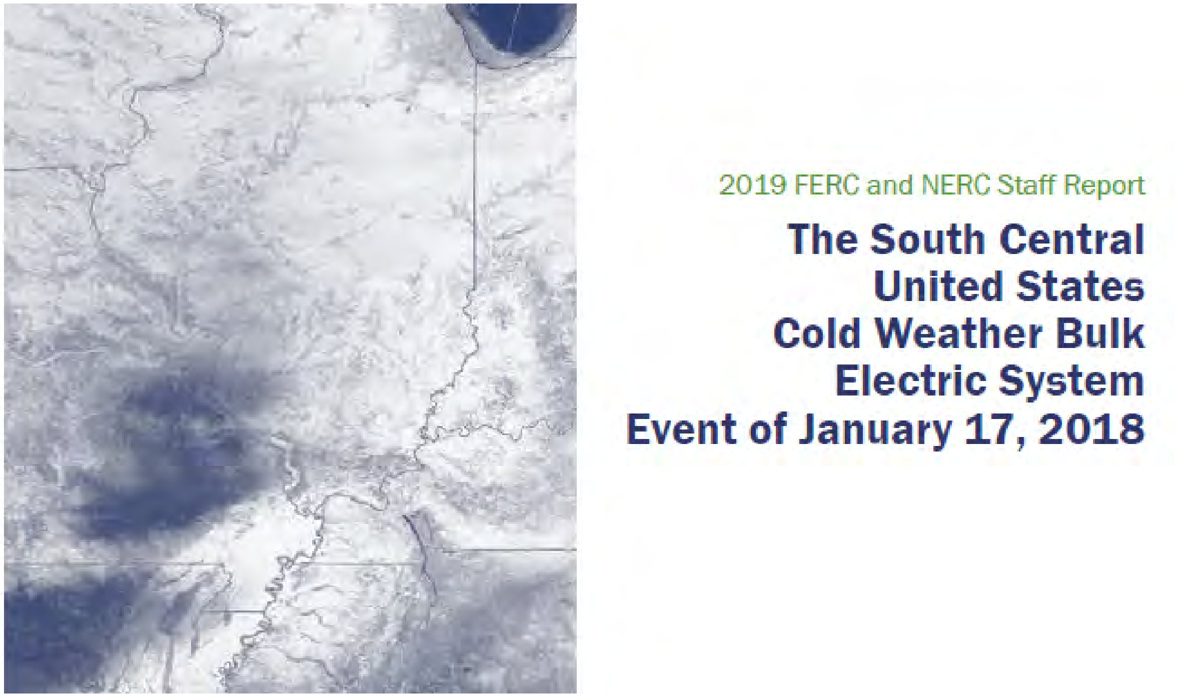
FERC and NERC Joint Report on Cold Weather Event

FERC and NERC recently released a joint report on the South Central U.S. Cold Weather Event of January 17, 2018. It stresses the need for generation owners and operators to adequately prepare for winter weather conditions to ensure bulk electric system reliability.

RF was pleased to be a part of the team and looks forward to continuing to work collaboratively to ensure cold weather preparedness.

In support of the recommendations in the Report, RF has been conducting Cold Weather Preparedness assessments since 2014. Cold weather readiness is key to ensuring reliability and resiliency, especially in the RF footprint which can get very cold winters. In recent years, RF has deployed cold weather readiness teams to visit select generating facilities and discuss best practices.

RF and NERC take the risk of Cold Weather Preparedness seriously and have developed Lessons Learned and Training Materials for Generation Owners and Operators. That important information can be found on our knowledge center here.



2019 FERC and NERC Staff Report

The South Central United States Cold Weather Bulk Electric System Event of January 17, 2018

Regulatory Affairs

RF President and CEO Tim Gallagher Participates in the FERC Reliability Technical Conference

On June 27, 2019, ReliabilityFirst President and CEO Tim Gallagher participated in the FERC Reliability Technical Conference. Mr. Gallagher presented on a panel entitled "Status of the Electric Reliability Organization and Reliability" with Jim Robb (President and CEO at NERC), Mark Lauby (Senior Vice President and Chief Reliability Officer at NERC), Jennifer Sterling (Vice President of NERC Compliance and Security at Exelon), Jack Cashin (Director, Policy Analysis and Reliability Standards at American Public Power Association), Nick Brown (President and CEO at SPP), and Peter Balash (Associate Director for Systems Engineering and Analysis - DOE National Energy Technology Lab).

Mr. Gallagher served as the Regional Entity representative on the panel and discussed how reliability and security risks can vary across the Regional Entities due to the Regions' unique geographical locations, electrical system configurations, and load densities. Because of these variations, the Regions conduct their own Regional Risk Assessments to prioritize the NERC Risk Elements present in each Region. Mr. Gallagher discussed how cyber and physical security are ERO-wide risks that are a major area of focus of the work being done by the Regions and by Registered Entities. He stressed the need to stay vigilant in identifying and mitigating cyber and physical security risks before those risks are realized as new risks continue to emerge. Another risk to the grid is extreme weather and he explained that after the polar vortex, ReliabilityFirst sent its own experts out into the field to perform winter weatherization visits at different plants and then disseminated lessons learned based off of those visits. Mr. Gallagher discussed outreach efforts such as Assist Visits, Workshops, and reports that have helped Registered Entities improve their CIP Compliance Programs. Mr. Gallagher also explained how the Regional Entities and NERC are focusing on both practicing and preaching continuous improvement. He further discussed how Reliability Standards are most appropriate for dealing with widespread and well understood risks that drive uniform performance across Registered Entities. Mr. Gallagher also stressed the risk of FERC releasing the names of Registered Entities that have major CIP violations too soon saying that "it's almost like there's a weakened animal in the herd and that's where all the lions are going to go" because some CIP violations take longer to correct even after mitigation is completed.

Other panels at the Reliability Technical Conference included discussions on the impact of cloud based services and virtualization on BES operations, planning, and security, reliability issues associated with Reliability Coordinator seams, and managing changes in communication technologies on the grid. The full conference can be watched at the following link.

NERC CEO Jim Robb Discusses Grid Security at House Committee Hearing on "Addressing Cyber Threats to the Grid"

The House Committee on Energy and Commerce invited Karen Evens, Assistant Secretary of the U.S. Department of Energy, J. Andrew Dodge, the Director of the Office of Electric Reliability at the Federal Energy Regulatory Commission, and Jim Robb, President and CEO of NERC, to discuss the security and reliability of the bulk power system. In his opening statement Jim Robb outlined the challenges facing the electric grid: "[t]he threat from cyber-attacks by nation states, terrorist groups, and criminals is at an all-time high. Now more than ever, grid security is inextricably linked to reliability."

The hearing centered on identifying government action which can assist the industry in further securing and improving the infrastructure of the electric grid. That is, what role Congress can play in terms of resource provision to aid the Department of Energy, FERC, and NERC. "The biggest issue for us, for NERC," Jim Robb said, "the most important thing from our perspective would be for government to be able to be more rapidly declassifying information to get it into actionable insights which we can take out to industry."

Karen Evans shared Robb's concern about information dissemination: "I would say that one of the biggest things that we need to do which you hit on, is making sure that dissemination of information and the sharing of the information hits at all levels."

As for preparation, the House Committee focused on the utility regulatory model, and whether the utilities were ready for the ratcheting up of cyber-interference from foreign countries and radical actors. "First I believe that the utilities are on a sort of constant alert," said Jim Robb, "because they know that they are a great attack target for foreign adversaries and are always on alert."

Both NERC and the Department of Energy emphasized the value of a potential tool and infrastructure certification program to protect against the use of easily infiltrated widgets in the electric grid. Robb said "[w]e think a supplier certification program is a very smart thing to do, the work the Department of Energy is doing in this area is terrific and there are some voluntary industry groups coming together to create a similar program."

Regulatory Affairs

U.S. Department of Energy, Office of Electricity to Develop Comprehensive Energy Map

By the end of 2019, the U.S. Department of Energy plans to develop a static computer model that maps the critical dependence of U.S. electricity generation on natural gas supplies. This first phase of a two-phase plan will produce a static model that is "a snapshot in time for different types of energy infrastructure that will enable [the DOE] to do analysis on the system," said Bruce Walker, the Assistant Energy Secretary and head of the DOE Office of Electricity. The Department of Energy received $24 million for Phase 1. The second phase of the plan will produce an interactive energy map of the United States and the energy system it shares with Canada and Mexico that would update a real-time model to show gas and electricity flows while also detailing outages and networks under stress. The DOE requested $30 million to develop the initial efforts on Phase 2.

This model is made possible by the natural gas industry members who volunteered to supply sensitive operating data needed for development. Some of the information provided by the electricity generators exceeds what grid operators are required to report. Designed by the DOE and its seven laboratories, the model includes data from renewable power generation, transmission flows, and the system maps of regional grid organizations. However, the remarkable increase of U.S. natural gas production over the last decade has made it the most important electric power plant fuel: it has displaced coal, reduced consumer costs, and lowered carbon emissions. This growing dependency on natural gas has the DOE concerned about just-in-time pipeline gas deliveries to power plants and the sector's vulnerability to terrorists, cyber threats, and major natural disasters. Although disruptions in the natural gas system can have serious consequences for electric power generation, gas pipeline outages are either not recorded or unavailable without a Freedom of Information Act request in most states, according to a 2018 study by researchers at Carnegie Mellon University and Vermont Law School.

Bruce Walker emphasized that the challenge is not collaboration across the industry, but rather obstacles created from big data analytics. There is real urgency among the DOE lab experts and their partners in academia to create information management systems at a rate faster than the data surge provided by new generators, micro-grids, customer power sources, and smart devices. The flood of connected technologies has expanded cybersecurity vulnerabilities. However, as of July 2019, the Federal Energy Regulatory Commission (FERC) has not acted on the 2018 docket, and the DOE is awaiting Congress to provide the funds. Walker concludes that "The situational awareness [of the new model] provides the ability to proactively mitigate, remediate, and eliminate risks, as well as to operate the system to optimize it for a variety of different things. The model could help operators have better visibility of emergency conditions to limit the damage."

Excerpted and summarized from Peter Behr and Jeremy Dillon, Electricity Chief on Gas, the Grid and 'Real-Time' Models, E&E News, July 25, 2019, here.

U.S. House of Representatives' Science, Space, and Technology Energy Subcommittee Explores Role of Artificial Intelligence to Improve Electric Grid Resilience

Because of the challenge confronting the DOE in analyzing and managing big data, Karen Evans, the Assistant Secretary for the DOE's Office of Cybersecurity, Energy Security and Emergency Response, testified on Wednesday, July 17th 2019 before the House Science, Space, and Technology Committee's Energy Subcommittee that Artificial Intelligence (AI) has a "critical role" in improving grid resilience. She explained: "We're talking about… software-defined networks, autonomous solutions, really analyzing the data… to remove some of what is happening at a human level now that could be done by AI, by machine learning. That is the area that we are really exploring so that we can look at higher analysis of security, and also being able to model the resilience in real time." Juan Torres, co-chair of the DOE's Grid Modernization Lab Consortium, agreed, explaining that the DOE is applying AI to four "foundational areas" of (1) understanding complex systems theory, (2) big data analytics, (3) optimization to ensure that distributed systems work together, and (4) non-linear controls. He added, "What we're seeing is with highly distributed systems, some of the linear control concepts that are used now on the grid may not apply in a highly decentralized type of system." Ultimately, AI would continue to build upon the smart grid technologies that have allowed the grid to operate with greater efficiency and transparency, as testified by Katherine Hamilton, Executive Director of the Advanced Energy Management Alliance. The four bipartisan bills that include focus and funding for the AI initiative passed the Energy and Commerce Committee by voice votes on Wednesday, and will be introduced to the full House after the August recess.

Excerpted and summarized from Rich Heidorn Jr., US House Takes on Grid Security, ERO Insider, July 21 2019, here.

Commissioner Cheryl LaFleur Leaves FERC

On July 18, 2019, Commissioner Cheryl LaFleur participated in her last public meeting as a member of FERC. When Commissioner LaFleur officially departs FERC in August, she will have served nearly ten years as a FERC Commissioner. Her tenure is the third-longest in FERC's history. During her time at FERC, she has served as Commissioner, Chairwoman, and acting Chairwoman. Commissioner LaFleur was first appointed by President Obama in 2010 and subsequently nominated again by him in 2014. Commissioner LaFleur's departure leaves two of FERC's five commissioner slots vacant. With three remaining Commissioners (two Republican and one Democrat), FERC still has the ability to issue decisions as FERC requires three Commissioners to constitute a quorum. ReliabilityFirst thanks Commissioner LaFleur for her service as a Commissioner and wishes her well in her next endeavors.

"Cheryl has been an outstanding and thoughtful public servant, contributor to reliability, security and resiliency, and friend. I wish her the very best as she moves forward." - Tim Gallagher.

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:

- Proposed Implementation Guidance:
  - CIP-012-1, R1 – Communications Between Control Centers (2016-02 SDT)
  - TOP-010-1 and IRO-018-1 – Real-time Assessment Quality of Analysis (OC)
  - CIP-008-6 – Incident Reporting and Response Planning (2018-02 SDT)
- ERO Enterprise-Endorsed Implementation Guidance:
  - CIP-013-1, R1, R2 – Supply Chain Management (NATF)

Reliability Standard Audit Worksheets Posted

NERC posted the following new Reliability Standard Audit Worksheets (RSAWs) are now available on the RSAW page under the heading “Current RSAWs for Use.”

- CIP-003-7 – Cyber Security – Security Management Controls applies to Balancing Authorities, Distribution Providers, Generator Operators, Generator Owners, Interchange Coordinators or Interchange Authorities, Reliability Coordinators, Transmission Operators, and Transmission Owners. The standard becomes effective on January 1, 2020.
- PRC-027-1 – Coordination of Protection Systems for Performance during Faults applies to Generator Owners, Transmission Owners, and applicable Distribution Providers. The standard becomes effective on October 1, 2020.
- The errata change for EOP-006-3 – System Restoration Coordination updates Part 8.1 to read “two calendar years” following the standard language. It applies to Reliability Coordinators.

Other Resources Posted

NERC has posted the following additional resources:

- The presentation and streaming webinar from the June 19, 2019 Substation Fires: Working with First Responders webinar.
- The presentations from the July 25, 2019 Electromagnetic Pulse Task Force Workshop.

Notable FERC Issuances

In June, FERC issued the following:

- Order Approving the Petition for the Request for Approval of Proposed Reliability Standard CIP-008-6
- Notice of Proposed Rulemaking Proposing to Approve Reliability Standard TPL-001-5

In July, FERC issued the following:

- Letter Order Approving Proposed Reliability Standard IRO-002-6
- Letter Order Approving Proposed Reliability Standard CIP-003-8

FERC’s issuances can be found here.

Notable NERC Filings

In June, NERC filed the following with FERC:

- Petition for Approval of Reliability Standards IRO-002-7, TOP-001-5, and VAR-001-6
- Petition for Approval of Standards Efficiency Review Retirements (INT, FAC, PRC, and MOD)
- Notice of Withdrawal of NERC for Proposed Reliability Standard MOD-001-2
- Comments of NERC in Response to Notice of Proposed Rulemaking on CIP-012-1

In July, NERC filed the following with FERC:

- 2019 Five-Year ERO Performance Assessment
- First Informational Filing of NERC Regarding Work Performed Under the Geomagnetic Disturbance Research Work Plan

NERC’s filings can be found here.

Standards Update

New Standards Projects

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

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

Recent and Upcoming Standards Enforcement Dates	
January 1, 2020	CIP-003-7 – Cyber Security – Security Management Controls; 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.

Fall Workshop
Cleveland, OH
October 1-3, 2019

The ReliabilityFirst 2019 Fall Workshop is fast approaching! We've compiled timely and important information for our stakeholders.

Day One

The reliability day will explore the rapidly transforming grid and what it means for reliability. We will have presentations from NERC, the DOE, and our reliability coordinators (PJM & MISO) and more experts from across the industry and RF on topics such as fuel security, long and short-term planning, event related disturbances, and distributed energy. We will also be tying all this back to what it means for reliability and conveying other reliability related information.

Day Two

The Compliance Users Group (CUG), and Critical Infrastructure Protection Committee (CIPC) meetings are held on the second day. Day three focuses on everything Cybersecurity and Critical Infrastructure with a keynote address from TrustedSec's David Kennedy, and presentations from the FBI, NERC, and ReliabilityFirst staff.

Day Three

Day three is on Cybersecurity and Critical Infrastructure and will have a keynote address from TrustedSec's David Kennedy and presentations from the FBI, NERC, and RF staff. There will also be a registered entity panel discussion regarding NERC CIP related issues and Lessons Learned.

A reminder that The Fall Workshop is being held on October 1-3, 2019 in Cleveland, OH at the Cleveland Marriott Downtown at Key Center. You can find the RF 2019 Fall Workshop agenda and hotel information here.

Registration will be open soon!

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

Duke Energy's Micro Grid Facility

RF and SERC employees, Bheshaj Krishnappa, David Sopata, Rick Dodd (SERC), Marty Sas (SERC) and Evan Shuvo (SERC) took a tour of Duke Energy's Micro Grid facility in Mount Holly, NC on July 11th 2019 .

The tour was presented by David Lawrence, Technology Development Manager at Duke Energy. The Mt. Holly facility is setup to experiment on real-time grid simulators, renewables, storage, electric vehicle charging, telecommunications, future technologies and cybersecurity.

The research done here helps Duke Energy to learn, how to deploy emerging technologies and make them reliable before they are commissioned in real world.

RF thanks David Lawrence for offering this tour to RF and SERC employees.

DUKE ENERGY
EMERGING TECHNOLOGY OFFICE
MOUNT HOLLY TRAINING CENTER
MICROGRID INNOVATION AREA

Watt's Up at RF

Protection System Workshop for Technical Personnel

August 13-14, 2019

Intended Audience

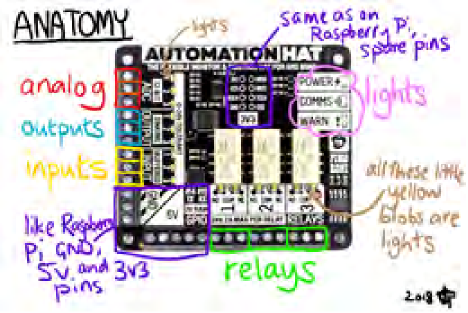
Substation Electricians/Supervisors Substation Field/Commissioning Engineers Relay Technicians

Relay Engineers and others who work Directly with this equipment

Communications Engineers/Technicians

Company Trainers on this Subject

Others interested in these topics


ANATOMY
lights
same as on Raspberry Pi, spare pins
AUTOMATION HAT
analog
outputs
inputs
lights
POWER
COMMS
WARN
all these little yellow blobs are lights
like Raspberry Pi GND, 5V and 3V3 pins
relays
2018

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**.”

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.

See You There!

Human Performance Workshop

August 14-15, 2019

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)

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.

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.

See You There!

Display Area for “Show and Tell” – NEW!

During these workshops, we will have an area with tables set up for anyone to bring something they would like to display for attendees to observe. Some suggestions are company human performance handbooks, relay technician HP kits, and any other materials your company may be willing to display that promote human performance excellence.

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
9/5	NERC Winter Preparation for Severe Cold Weather Webinar
9/10-9/11	FERC Technical Conference regarding Managing Transmission Line Ratings (Docket No. AD19-15-000) (Washington, DC)
9/19	FERC Open Meeting
9/24-9/25	NERC Monitoring and Situational Awareness Technical Conference, Little Rock, AR
10/17	FERC Open Meeting
10/22-10/24	NERC TADS Conventional Training, Atlanta, GA
11/21	FERC Open Meeting
12/10-12/11	FERC Environmental Review and Compliance for Natural Gas Facilities Seminar (Seattle, Washington)
12/19	FERC Open Meeting

Ohio Passes House Bill 6

On July 23, 2019, Ohio Governor Mike DeWine signed House Bill 6 into law. The bill provides $150 million in annual subsidies for FirstEnergy's Davis-Besse and Perry nuclear plants. The bill changes Ohio's 12.5% renewable energy standard to 8.5%. The bill also sets aside $20 million for the development of utility-scale solar projects. Opponents of House Bill 6 have pledged to seek enough petition signatures to force a referendum to overturn House Bill 6 in November 2020.

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