Issue 6
2019 November/December

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,

As weather gets colder and days get dark earlier, the importance and dynamic nature of our work becomes more noticeable. These tangible reminders of change are paving the way for more than just a New Year – we are entering a new decade. Before kicking off what I'm sure will be an exciting and successful 2020, I'd like to pause and share my gratitude.

On behalf of the entire RF staff, we appreciate your many contributions to ensuring the reliability and security of the BPS. Without the hard work and dedication of everyone in our Region and across the ERO, we could not have ended 2019 on such a positive note. This year has been incredibly encouraging, largely due to the widespread enthusiasm and support for the ERO's new strategic vision and alignment among NERC and the Regions.

This last quarter has capped off the year with even more forward momentum. The NERC working group meetings in Atlanta were filled with valuable insights and innovative ideas for future collaboration; GridEx V identified opportunities for continuous improvement in the face of new and evolving challenges; and our final Board Meeting of the year and Annual Meeting of Members in Washington, D.C. reinforced my belief that, with our collective efforts, we are more prepared than ever for the future.

A final note of gratitude during this season of change is our sincere thanks to Ken Capps for his service and commitment to RF's mission during his tenure on our Board of Directors. He served as an at-large member since the Board's beginning, and his leadership will be missed. Ken served as Board Chair, Vice-Chair and Board Compensation Committee Chair during his time with us, not to mention the guidance, wisdom, knowledge and friendship he shared with me personally and with all in the organization during the past 14 years.

I'm already looking forward to seeing many of you here in Cleveland soon at our first-ever Internal Controls Workshop on Feb. 12, which will be followed by the CIPC Meeting the next day.

Until then, please accept my warmest wishes for a wonderful holiday season with your loved ones and a New Year filled with health and happiness.

Forward Together,

Tim

From the Board

Annual Meeting of Members, Fourth Quarter Board of Directors and Committee Meetings

Robert Clarke

ReliabilityFirst was honored to have Robert Clarke and Andy Dodge as the keynote speakers during the 2019 Annual Meeting of Members and Fourth Quarter Board of Directors meetings in Washington, DC. Robert Clarke, member of the NERC Board of Trustees, provided the keynote address at the Annual Meeting of Members. He discussed the ERO Enterprise's new strategic vision and the collaborative approach among NERC and the Regions. Mr. Clarke also discussed key areas of focus for the ERO Enterprise, including E-ISAC expansion and a continued emphasis on risk identification and mitigation activities.

Andy Dodge

Andy Dodge, Director of the Office of Electric Reliability at FERC, provided the keynote remarks at the Fourth Quarter Board meeting. He discussed the reliability challenges associated with the changing resource mix and extreme weather conditions. He also recapped and discussed recent events involving inverter based resources, fuel assurance, and extreme cold weather impacts. Mr. Dodge then discussed the role of reliability Standards in responding to these reliability challenges. He stressed that complete, accurate, and validated models are essential to reliability, and stated the value of going beyond baseline compliance to identify solutions for individual and regional challenges and risks.

RF Thanks and Recognizes Departing Board Member Ken Capps

Lisa Barton, Ken Capps and Tim Gallagher

During the Fourth Quarter Board Meeting, RF recognized the service of Ken Capps, whose term expired this year. Tim Gallagher, President and CEO, and Lisa Barton, Board Chair, thanked Mr. Capps for his service and leadership during his tenure. Mr. Capps served as an at-large member on ReliabilityFirst's Board since its inception. He recently retired from his position as Senior Vice President and Chief Operating Officer for Southern Maryland Electric Cooperative, Inc. (SMECO), a non-profit electric distribution cooperative serving nearly 150,000 members in the Charles, St. Mary's, Calvert and Prince George's counties of Maryland.

Lisa Barton Concludes Term as Board Chair

Lisa Barton's term as Chair of the Board expired this year. She has served as RF's Board Chair since December 2017 and has been a member of the Board since 2014. Tim Gallagher thanked Ms. Barton for her service and leadership, and noted that she will continue in her role as a director representing the Supplier Sector.

Ms. Barton is the Executive Vice President – Utilities at American Electric Power Service Corporation (AEP) overseeing AEP's seven operating companies with electric generation, transmission and distribution operations in 11 states. Previously, Ms. Barton served as Executive Vice President Transmission, President and COO, AEPTHC. Ms. Barton earned a bachelor's degree in electrical engineering from Worcester Polytechnic Institute and a juris doctorate degree from Suffolk University Law School. She is a member of the New Hampshire Bar, Massachusetts Bar, and is admitted to practice before the U.S. Patent and Trademark Office. She was an International Women's Foundation Fellow, member of G100 Next Generation Leadership and is a member of C200.

RF Announces New Board Leadership

RF is pleased to announce that Simon Whitelocke will serve as its new Board Chair, and Lynnae Wilson will serve as its new Board Vice Chair.

Simon Whitelocke

Mr. Whitelocke is Vice President of ITC Holdings Corp. and President of ITC Michigan, which includes the responsibility for both ITC Transmission and METC operating companies. Prior to this role, he was Vice President and Chief Compliance Officer for ITC Holdings Corp. where he was responsible for the corporate compliance functions of the company. Mr. Whitelocke also has served in other roles responsible for regulatory affairs, external affairs and internal audit functions. Prior to joining ITC, he was a Principal Financial Consultant for DTE Energy. Mr. Whitelocke earned a Bachelor of Commerce degree in accounting from the University of Toronto and an MBA in finance and management from Michigan State University. He is also a member of the Board of Trustees of Detroit Public Television, and the Board of Trustees of Legacy Land Conservancy.

Lynnae Wilson

Ms. Wilson is Chief Business Officer, serving as Indiana Electric Lead for CenterPoint Energy. She is responsible for power generation operations and construction, electric transmission and distribution operations, electric engineering and oversees Midwest Independent System Operator (MISO) engagement which includes wholesale power marketing. Ms. Wilson has more than 15 years of experience in combined natural gas and electric utilities and electric generation with Vectren, in addition to experience in the manufacturing and mining industries. She is a board member and former Board President and Vice President for Mental Health America of Vanderburgh County, Indiana. Lynnae is a graduate of Missouri University of Science and Technology, where she earned her bachelor's degree in mining engineering.

Get Control of Yourself!

By Denise Hunter, Principal Technical Auditor

Can you believe how quickly this year has flown by? Before you know it, it will be time to attend the **RF Internal Controls Workshop**! (I bet you thought I was going to say Christmas.) Here is my shameless plug: the workshop is Wednesday, Feb. 12, 2020 in Cleveland, and you can register here. This truly will be a working session where your company's SME and PCC will work to capture your company-specific internal controls for two Standards, one O&P and one CIP. The O&P Standard will be PRC-004-5(i). Therefore, I will continue with that subject in this issue and address the ERO risk element **Improper Determination of Misoperations**.

In order to dive into this subject, we need to have a common understanding of the risk presented by this ERO risk element. This risk lies in a number of areas, and some ERO documents have identified a few:

1) According to the 2019 Compliance Monitoring and Enforcement Program Implementation Plan,[1] "When protection systems are not coordinated properly, the order of execution can result in either incorrect elements being removed from service or more elements being removed than necessary."

2) The 2018 ERO Reliability Risk Priorities report [2] identifies in its Risk Profile #4: Increasing Complexity in Protection and Control Systems, that improper coordination of control system assets could negatively affect the resiliency of the BES due to control system misoperations or failures.

3) Additionally, I would offer that we also must include the coordination of operations, as well as lack of appropriate internal controls, tools, data, services and personnel necessary, to ensure the reliability of the BES.

When you consider the number of moving parts that could initiate a misoperation, it is understandable (and not lost on RF) how challenging a task it might be to determine the true cause. Regardless and however daunting the process might be, a strong internal control can reduce improper determinations of misoperations.

Before beginning the process of identifying possible internal controls that might help reduce improper determinations, and a few controls that could possibly help mitigate the possibility of a misoperation, let us review some facts from a few events. Specifically, let us examine the Arizona-Southern California Outages [3] and the Aug. 14, 2003 Blackout [4]. Additionally, some information from the NERC 2013 and 2019 State of Reliability (SOR) reports and the 2018 RISC Recommendations to the NERC Board of Trustee's report could prove useful in this review.

Arizona-Southern California VS August 14, 2003 Blackout

The Arizona-Southern California Outages Sept. 8, 2011 report noted a number of common underlying causes between that outage and the Aug. 14, 2003 Blackout. First, "both reports described relevant planning studies that:

(1) did not adequately identify and study critical external facilities;

(2) did not adequately analyze potential contingency scenarios; and

(3) were based on inaccurate models and invalid system operating limits (SOLs)."

Second, "in both events, the affected entities' real-time monitoring tools were not adequate to alert operators to system conditions and contingencies. In addition, some of the affected entities in both events did not use their real-time tools to monitor system conditions. As a result of these situational awareness issues, affected entities in both events were not aware that they were no longer operating in a secure N-1 state and were not alerted to the need to take corrective actions."

NERC 2013 and 2019 State of Reliability Report(s)

Next, the NERC SOR 2013 [5] (reporting on 2012 activity) identified that the main causes for misoperations are from incorrect settings/logic/design errors, communication failure, and relay failure or malfunction. (See Figure 1.6.)

[1] 2019 CMEP IP, pg 20

[2] [See2018 RISC Recommendations to the NERC BoT

[3] [See Arizona-Southern California Outages Sept 8, 2011

[4] See August 14, 2003 Blackout Final report

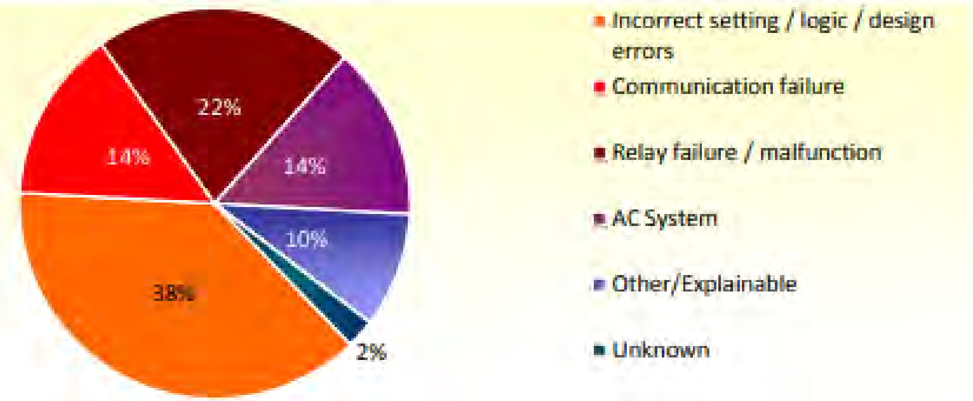
[5] NERC State of Reliability 2013

Continued on page 4

Get Control of Yourself!

Continued from page 3

Figure 1.6: Misoperations in 2012 Cause-Coded Disturbance Events (42 Misoperations within 33 Qualified Events)



The NERC SOR from 2019[6] noted the same three largest causes of misoperations. (See Figure 5.5.)

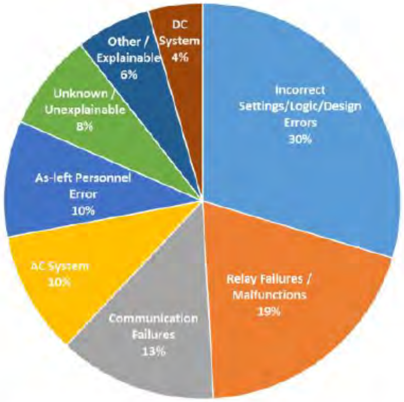


Figure 5.5: Misoperations by Cause Code (4Q 2013 through 3Q 2018)

Let us stop for a minute and look at those facts. How is it possible that issues identified in 2003 still prevailed eight years later? Moreover, how is it that the main causes for misoperations identified in 2012 remain the most common causes in 2018? Perhaps we need to look at these activities in a different light.

To recap, misoperations are sometimes due to protection systems being improperly coordinated; and the three main causes of misoperations have consistently been setting/logic/design errors, communication errors, and relay failures or malfunctions. We also learned that these problems have prevailed over the years. Based on that information, the next question begs "What exactly does proper coordination entail?" At the most basic, it is "the harmonious functioning of parts for effective results, the proper order or relationship, harmonious combination or interaction, as of function or parts." [7] Before dissecting what controls might help mitigate the risk of not being properly coordinated, let us review a few recommendations that were presented in the reports mentioned above.

Recommendations and Risk Based Compliance

Each of the reports noted in this article provided recommendations regarding misoperations and ideas to reduce them. Historically, these recommendations (taken directly from the NERC 2019 SOR and the 2018 RISC report) focused on areas such as:

1) Detailed data reporting instructions (DRI) for misoperations to create better alignment of entity understanding and more consistent submissions of misoperation data;

2) Expanded efforts on education, outreach and training;

3) Determining whether enhancements are required to the current family of protection and control (PRC) standards or related NERC guidance materials; and

4) Encouraging industry forums, research organizations and technical committees to share technologies or processes on condition monitoring, failure prevention, spare sharing, resilience and recovery.

[6] NERC State of Reliability 2019

[7] Merriam-Webster dictionary

Continued on page 5

Get Control of Yourself!

Continued from page 4

These are all great recommendations—however, I would like to offer a few more suggestions, specifically a few controls, which might help.

Let's get started with the controls!

The first of these controls speaks directly to the ERO risk element of Improper Determination of Misoperations. The NERC Cause Analysis methods for NERC, Regional Entities and Registered Entities [8] defines a strong incident management control. This control outlines the process of analyzing and reporting on the cause of an event.

The methodology:

1) Outlines the analysis process from data collection and the type of data collected;

2) Reviews the data and how it is assessed;

3) Identifies corrective actions, reporting and following up;

4) Describes a systematic process to identify the appropriate root cause analysis method to use, based on specific criteria;

5) Addresses team composition; and

6) Includes risk presented by Human Performance factor.

This control appears thorough and complete, and when followed should produce the desired product: a clear identification of the cause of an event.

However, I would like to provide a recommendation for the performance of this control. Section 3.5.3 Team Composition states, "The majority of human performance errors and equipment failures are investigated by one or two subject matter experts." The size of the team can sometimes present its own risks. If the team is too small, the investigation could lack the expertise and historical knowledge gained from a diverse, larger team and suffer from cognitive bias. Although, research has identified that smaller teams (less than three members) tend to be more disruptive. "Analyses uncovered a nearly universal pattern: whereas large teams tended to develop and further existing ideas and designs, their smaller counterparts tended to disrupt current ways of thinking with new ideas, inventions, and opportunities." [9] Small teams can produce just as well as larger counterparts, but I would caution that smaller teams present different risks (i.e., cognitive bias) that must be mitigated with secondary controls.[3] I suggest that anytime there are critical, technical steps performed, there should be consideration for segregation of duties.[4] If that is not possible, then a review should be performed by a knowledgeable second party, following key steps.

Next, I would like to offer some controls that could help mitigate the occurrence of a misoperation.

Based on the previously identified reoccurring causes, a defined Coordination Control should be considered. A well-defined Coordination Control is organized in multiple layers that integrate the operations of subsystems into one functioning system. It involves establishing lists of inputs and outputs that affect risks to grid reliability and brings subsystems, or components of a subsystem, together into one system. The aggregation of subsystems works together so that the system performs the overarching functionality.

When defining a Coordination Control, considerations should include:

1) Formulating the concept of coordination through identification of the various internal and external interfaces affecting an organization. Consideration might need to include areas outside the BPS (i.e., possible operations of external network facilities or the reliability of sub-100 kV facilities).

2) Ensuring appropriate communication, cooperation and coordination across all affected parties and planning horizons in order to build a distributed system and develop control synthesis for the coordinated systems.

3) Documenting the internal and external interfaces and the steps required for successful coordination.

4) Verifying and validating the design to ensure it functions correctly and as designed.

5) Identifying a strong Change Management process that properly addresses any changes that affect the control, including emergency conditions. (See my article on Gaps in Program Execution for a detailed discussion on a Change Management control.)

6) Establishing monitoring activities at the department level to be performed at risk-determined intervals.

[8] NERC Cause Analysis Methodology

[9] https://hbr.org/2019/02/research-when-small-teams-are-better-than-big-ones

[10] Secondary Control: An important control that typically takes place after the process it applies to (i.e., reconciliations or reviews) and could be replaced by monitoring. See the RF Knowledge Center/Internal Controls/Internal Control Program & Activities/Internal Control Flashcards

[11] Segregation of Duties: Based on shared responsibilities of a key process, disperse the critical functions of that process to more than one person or department.

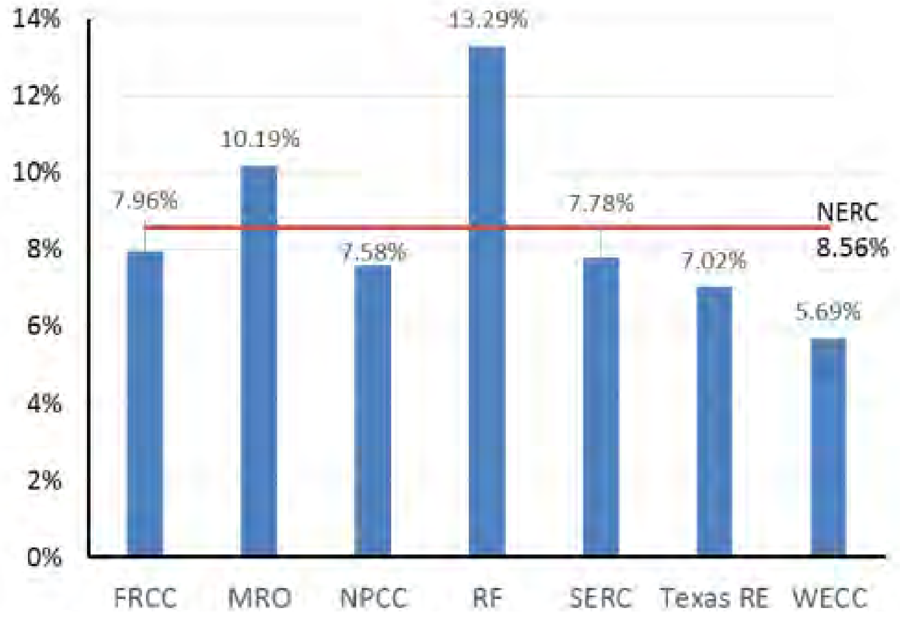
Continued on page 6

Get Control of Yourself!

Continued from page 5

I believe a well-defined Coordination Control is a great first step toward reducing misoperations. However, that alone is not enough. To that end, RF has conducted numerous outreach activities over the years. These include conferences regarding technical aspects of misoperations; training sessions for communication technicians, field personnel and relay engineers; technical sessions on power line carrier equipment and issues; and human performance seminars, to name a few. All of these efforts have made progress in moving the needle in the right direction. (See SOR 2019 Figure 3.2.) Still, I believe designing, implementing and monitoring the appropriate controls will help improve those numbers even more.

Figure 3.20: Five-Year Protection System Misoperation Rate by Region Q4 2013 through Q3 2018



A peer review of protection system design and its applicable settings could be a good place to start—especially considering that it is the highest cause of misoperations in our region. This is not a difficult control to implement and would consist of an independent review of protection system design and the settings, during both the design phase and commissioning phase. This control should be a methodical review that systematically analyzes and appraises the data, while adhering to guidelines on the conduct of the review.

As stated in my article on Gaps in Program Execution, verification of your asset listing could mitigate a large risk to the BES. It warrants repeating because incorrect asset listings due to component replacements, setting changes, human error, etc. do occur, placing the reliability of the BES at risk. The risk of not performing this control could place any other controls established around asset performance and asset maintenance in a suspect position. Attacking this issue systematically by establishing a schedule that does not place your entity under undue stress would go a long way in ensuring your reliability to the BES. As in the old “eating an elephant” metaphor, it helps to approach this one bite at a time.

Additionally, in order to maintain an established baseline and all applicable supporting documentation accurately, a strong Change Management control is necessary. The settings/logic/design may be high because the relay settings were correct and reviewed when they were set, but as the system changed (due to fault current changed, generation retired, new substations/lines, etc.), the existing settings/logic/design was no longer ideal. The change itself is not the only challenge—it is all the other systems that the change could impact, such as relay settings busses away. A strong Change Management control addresses and updates all the systems affected by a change.

Finally, I suggest standardized forms to help when designing protection schemes. Considering this process includes obtaining information such as impedance of line information and technical data for the assets, standardized forms could help mitigate the risk of inaccurate or incomplete information. Standardized forms assist a process through familiarity of the form, less deviation from expected information, and higher confidence that all required information is included.

Statistically speaking, the next event is coming, and without the appropriate controls defined, implemented and monitored, the result may not be much different.

Until next time, stay warm and I hope to see you at the Internal Controls Workshop in February where RF will be facilitating the process of documenting your PRC-004-5(i) controls!

Insider Threats - HR and Legal, Part 5

By Bhesh Krishnappa, Program Manager, Risk & Resiliency

Program Management
Personnel & Training
Collection & Analysis
HR & Legal
Insider Threat Program

In the previous Insider Threats articles, we discussed setting up an Insider Threat Program (ITP) including hiring relevant personnel for the program, conducting required training, and data collection and analysis to detect insider threat events. In this concluding article in the series, we will explore the role human resources (HR) and Legal personnel have in instituting and running a successful ITP.

Human Resources

HR is already the driving force behind hiring the right people for each role. As part of NERC Standards compliance management, this includes tasks like performing personnel risk assessments periodically for employees, contractors or service vendors. The Standards directly responsible for such activities are CIP-004-6 Table R3 – Personnel Risk Assessment Program and CIP-004-6 Table R5 – Access Revocation.

HR's role encompasses reviewing insider threat policies and processes, as well as executing relevant internal communications and training. Also, HR can take the lead in setting up programs for employees to seek assistance within the organization to openly discuss work-related issues with management or HR staff without fear of reprisal or negative consequences. A positive and open communication forum can help employees or contractors strengthen the ITP, particularly in terms of detecting potential insider threats and activity.

In addition, HR has access to sensitive or confidential information about employees' performance which may help in detecting potential malicious insider threat activity. HR has knowledge of all personnel reassignments, transfers or terminations, which gives them the opportunity to provide the insider threat team with an automated or manual listing of these changes. Sometimes it is necessary to implement additional actions (such as involving law enforcement) as a result of terminations to deter malicious activity in advance.

Legal

Like HR, Legal should be included in all aspects of developing and operating an ITP. Legal helps balance security and user privacy while navigating the legal aspects of ensuring insider threats are mitigated effectively. According to the article titled "Insider Threat Legalese," [a] some of the types of laws applicable to insider threats are:

- Compliance – ITP development and regulatory compliance
- Intellectual property – asset protection and program development
- Employment law – background checks, employment decisions, employment agreements and monitoring
- Cybersecurity law – breach notification and incident response
- Privacy law – collecting, processing, storing and disseminating personal information
- Criminal law – liaising with law enforcement, economic espionage and theft of trade secrets
- Civil litigation – enforcing covenants, NDAs and obtaining injunctions

Some privacy laws span across state and national boundaries to protect the civil liberties and privacy of all stakeholders involved in operating and maintaining energy critical infrastructure. For example, some states, such as Maryland, [b] have explicit laws prohibiting employers from requesting social media passwords or accessing the social media accounts of prospective and current employees; whereas some states are yet to develop such laws. These types of background checks or social media information are accessed prior to employment or as a part of ongoing user activity monitoring.

Further, Legal and HR can help in instituting policies and procedures for identifying and managing employees considered to be a risk. This can depend on the level of physical and electronic access an employee has to the BES facilities. Adequate response options included in the policy help responses align with privacy protection requirements and other policies in effect.

ITP mandates that intellectual property is handled accordingly. In the electricity sector, NERC CIP-011-2 Cyber Security - Information Protection Standard mandates protecting critical BES Cyber System Information (CSI) against compromise. This involves identifying, protecting and securely handling BES CSI, including storage, transit and use of such data. This Standard, along with CIP-004-6 Table R4 – Access Management Program, can help strengthen access to critical information, either electronic or physical, to ensure BES assets are adequately protected.

Finally, it is important that all stakeholders involved in ITP management are familiar with the insider threat policies, identification, and coordination and response options. Legal and HR play a particularly significant role in ensuring disgruntled employee are handled appropriately. An organization should strive for good communication of policies and procedures to minimize employee disruption and dissatisfaction during triggers such as a restructuring process, office relocation, promotions, etc.

Effective use of technical and process controls can address insider threat mitigation in a timely manner. Segregation of duties, access on a need-to-know basis, and timely revocation of unnecessary access are examples of technical

Continued on page 8

Insider Threats - HR and Legal, Part 5

Continued from page 7

controls. Process controls, like effective communication around training, motivating employees, and employee assistance programs, have proved effective.

As noted in previous articles, there are several free resources available for setting up an ITP or creating awareness in your organization. Some of the valuable resources which may help are listed below for reference:

1. Common Sense Guide to Mitigating Insider Threats, Fifth Edition – (free download)
2. SEI Training - CERT Insider Threat Program Evaluator/Manager Certificate or CERT Insider Threat Vulnerability Assessor Certificate
3. Government's Center for Development of Security Excellence
4. Free Insider Threat Vigilance Campaign Materials
5. Insider Threat Toolkit
6. Insider Threat to Cyber Security – Kate Randall, FBI Insider Threat Analyst (example of using narcissism as a potential indicator among FBI special agents)
7. Insider Threats: Your Questions. Our Answers
8. Effective Insider Threat Programs: Understanding and Avoiding Potential Pitfalls
9. The Critical Role of Positive Incentives for Reducing Insider Threats

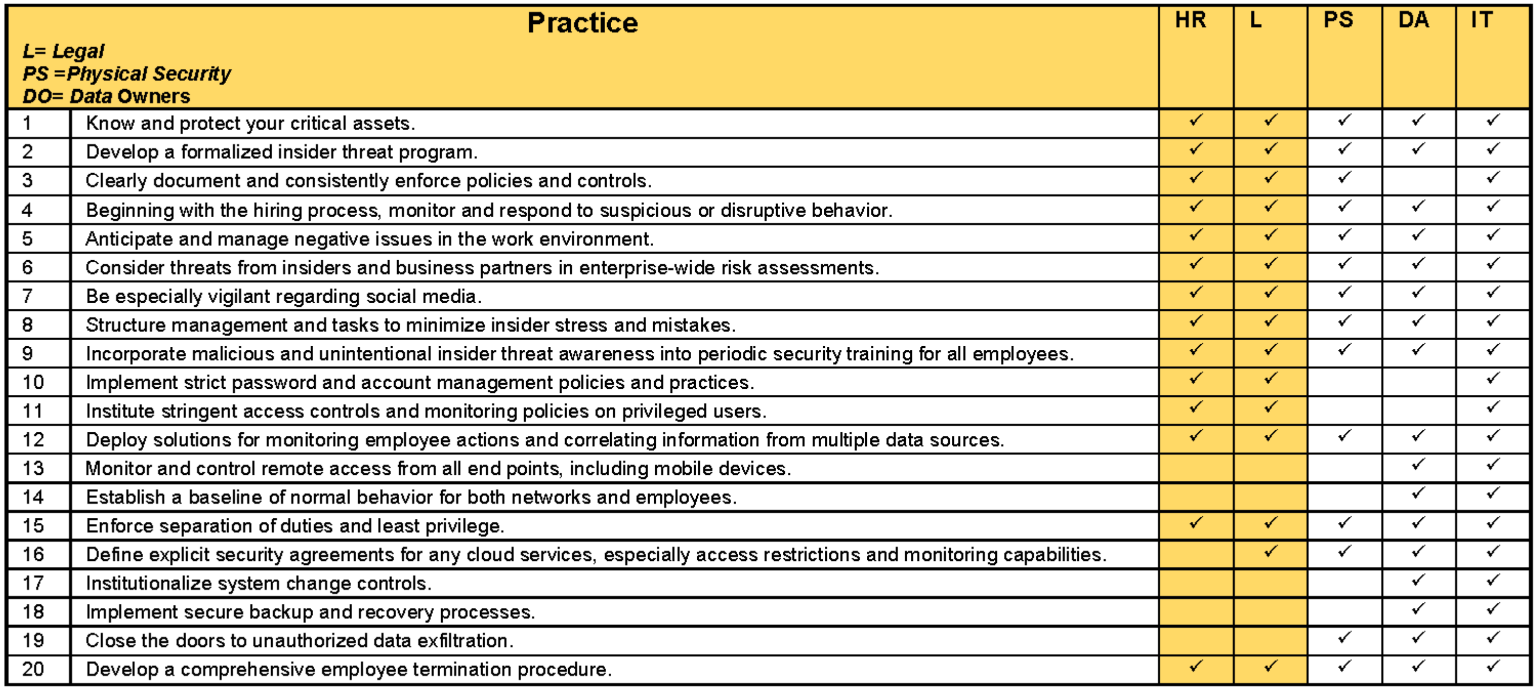
Additional resources from DHS:

10. Insider Threat Mitigation
11. Insider Threat Mitigation Program Available Resources
12. Insider Threat Trailer and Video
13. Pathway to Violence Video
14. IS-915: Protecting Critical Infrastructure Against Insider Threats course (free)

References in the article::

a. "Insider Threat Legalese"
b. Maryland

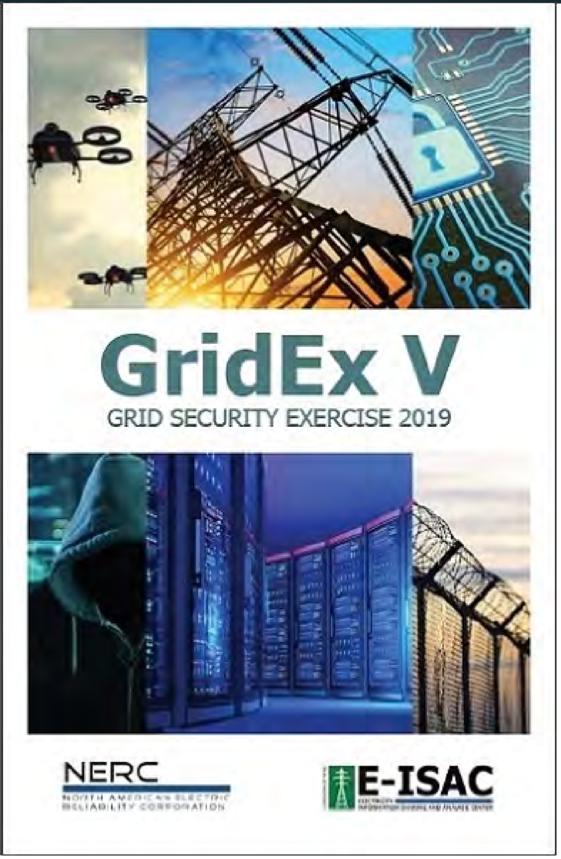
The table below is from the SEI CERT Common Sense Guide to Mitigating Insider Threats, Fifth Edition and notes some best practices for all organizational groups.



Practice *L= Legal* *PS =Physical Security* *DO= Data Owners*		HR	L	PS	DA	IT
1	Know and protect your critical assets.	✓	✓	✓	✓	✓
2	Develop a formalized insider threat program.	✓	✓	✓	✓	✓
3	Clearly document and consistently enforce policies and controls.	✓	✓	✓		✓
4	Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.	✓	✓	✓	✓	✓
5	Anticipate and manage negative issues in the work environment.	✓	✓	✓	✓	✓
6	Consider threats from insiders and business partners in enterprise-wide risk assessments.	✓	✓	✓	✓	✓
7	Be especially vigilant regarding social media.	✓	✓	✓	✓	✓
8	Structure management and tasks to minimize insider stress and mistakes.	✓	✓	✓	✓	✓
9	Incorporate malicious and unintentional insider threat awareness into periodic security training for all employees.	✓	✓	✓	✓	✓
10	Implement strict password and account management policies and practices.	✓	✓			✓
11	Institute stringent access controls and monitoring policies on privileged users.	✓	✓			✓
12	Deploy solutions for monitoring employee actions and correlating information from multiple data sources.	✓	✓	✓	✓	✓
13	Monitor and control remote access from all end points, including mobile devices.				✓	✓
14	Establish a baseline of normal behavior for both networks and employees.				✓	✓
15	Enforce separation of duties and least privilege.	✓	✓	✓	✓	✓
16	Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.		✓	✓	✓	✓
17	Institutionalize system change controls.				✓	✓
18	Implement secure backup and recovery processes.				✓	✓
19	Close the doors to unauthorized data exfiltration.			✓	✓	✓
20	Develop a comprehensive employee termination procedure.	✓	✓	✓	✓	✓

RF Participates in GridEx V

By David Sopata, Principal Reliability Consultant


GridEx V
GRID SECURITY EXERCISE 2019
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
E-ISAC

The overall mission of the GridEx exercise, hosted by NERC and E-ISAC, is to improve Registered Entities' and government agencies' incident response plans against catastrophic physical and cyber security events. It is completely voluntary, non-compliance binding and includes representatives of the electric utility industry, other interdependent infrastructures (such as gas, water and telecommunications), and government organizations in North America.

The GridEx Working Group developed the Master Scenario Event List (MSEL) and the supporting inject materials to provide a more customizable, interactive, realistic and hands-on experience for participants. Entities can customize the MSEL to be more of a high-level tabletop, but they are encouraged to make it as interactive and realistic as possible using the same tools and systems that they would use in real situations.

Entities are encouraged to develop their own injects to help them assess against other types of unique threats or potential risks to their operations. From these exercises, lessons learned are captured and shared to help strengthen internal response and recovery procedures, improve internal and external communication and coordination, and help improve GridEx to make it a better experience in the future.

Started in 2011, GridEx is a biennial event. This timing allows for a planning year and an execution year, which makes it one of the most thoroughly planned, coordinated and relevant tabletop exercises for critical infrastructure with a focus on the Bulk Power Grid. GridEx V occurred Nov. 13-14 of this year and involved more than 5,000 registered participants from more than 450 different organizations. The theme for GridEx V was interdependencies. Entities were encouraged to invite and coordinate with local and regional government, law enforcement, other interdependent critical infrastructures (such as water and gas), and third party suppliers and vendors who would be needed during recovery efforts. Many of the organizations, such as Registered Entities, Utilities, RTOs, Regional Entities, Department of Energy, Department of Homeland Security, FBI, Department of Defense, and state and local governments, actively participated throughout the exercise by responding to the events, while others observed.

RF has been an active member of GridEx since its start back in 2011. RF not only helps in the planning and the development of the MSEL in the GridEx Working Group, but participates in the exercise as well. This year, custom injects were developed for RF's Event Analysis and Situational Awareness (EASA), information technology (IT) and corporate communications teams to help assess internal processes and procedures for internal physical and cyber threats, BES event analysis and situational awareness, and emergency communications and procedures.

Throughout the two-day event, RF collaborated with NERC staff, RTOs and Registered Entities to understand and assess the impacts of the simulated events to the RF footprint and to identify how RF could assist in response to the events unfolding. The IT team also dealt with their own set of simulated attacks requiring additional actions to protect and respond to threats against their operations and protected data.

Going forward, RF will participate in NERC-led discussions to capture lessons learned across the ERO. Those lessons, as well as our own internal lessons learned, will be incorporated into continuous improvement efforts for our internal processes and procedures.

We remain dedicated to working with others within the ERO to improve communications between and among NERC, the Regional Entities and the Registered Entities with the goal that we are all better prepared for the possibility of a real event of the magnitude simulated in GridEx V.

2020 O&P Spot Checks for Generator Owners and Operators

For a number of years, ReliabilityFirst has implemented risk-based compliance monitoring. Risk-based compliance monitoring has several advantages—the primary one being that it enables RF and our Registered Entities to focus on the higher risks associated with particular Standards/Requirements.

This article discusses some of the risk-based compliance monitoring that RF will implement in 2020 for certain Operations and Planning (O&P) Standards/Requirements that are applicable to selected Generator Owners (GOs) and Generator Operators (GOPs). It also reviews the risks associated with these Standards/Requirements and provides some guidance for applicable Registered Entities to consider when preparing for the monitoring.

Spot Check Scope

RF will conduct Spot Checks of the following Standards/Requirements that are applicable to GOs:

· MOD-025-2 (Verification and Data Reporting of Generator Real and Reactive Power Capability and Synchronous Condenser Reactive Power Capability) Requirements 1 & 2

· PRC-019-2 (Coordination of Generating Unit or Plant Capabilities, Voltage Regulating Controls, and Protection) Requirement 1

· PRC-024-2 (Generator Frequency and Voltage Protective Relay Settings) Requirements 1 & 2

RF will conduct Spot Checks of the following Standard/Requirement that are applicable to GOPs:

· VAR-002-4.1 (Generator Operation for Maintaining Network Voltage Schedules) Requirement 2

Risks

The risks associated with the above Standards/Requirements include:

· Insufficient long-term and operations planning/analysis due to inadequate models from a failure to verify or report generator Real and Reactive Power capabilities (MOD-025-2), or a failure to communicate regulatory or equipment limitations that may result in a generating unit tripping during a voltage or frequency excursion (PRC-024-2).

· Unnecessary unit trips or equipment damage resulting from a lack of coordination of voltage regulating system controls with the applicable equipment capabilities and settings of the applicable Protection System devices and functions (PRC-019-2)

· Unnecessary unit trips during frequency or voltage excursions resulting from frequency or voltage relays not being properly set (PRC-024-2).

· Improper voltage levels (with the potential for voltage collapse) resulting from not maintaining generator voltage or Reactive Power schedules, or not complying with instructions to modify voltage (VAR-002-4.1).

MOD-025-2 Guidance and Expectations

· The Standard has a phased-in Implementation Plan.

· Per the Implementation Plan, 100% of applicable Facilities were to be verified by July 1, 2019.

· The first verification must be a staged test.

· New applicable Facility must be verified within 12 calendar months of its commercial operation date.

· Ensure that the verifications are performed per Attachment 1 of the Standard.

· Ensure the completed Attachment 2, or a form containing the same information as identified in Attachment 2, includes a representative one-line diagram and ALL of the data/information listed.

· Ensure Attachment 2 is submitted to the correct Transmission Planner within the required time.

· Each applicable Facility must be verified at least every five years (with no more than 66 calendar months between verifications), or within 12 calendar months of the discovery of a change that affects its Real Power or Reactive Power capability by more than 10% of the last reported verified capability and is expected to last more than six months.

PRC-019-2 Guidance and Expectations

· The Standard has a phased-in Implementation Plan.

Continued on page 11

2020 O&P Spot Checks for Generator Owners and Operators

Continued from page 10

· Per the Implementation Plan, 100% of applicable Facilities were to be coordinated by July 1, 2019.

· New applicable Facilities must be coordinated by the time they are placed in service (i.e., interconnected).

· Reference Section G for equipment limits, types of limiters and protection functions which could be coordinated.

· Provide a list of in-service limiters and applicable in-service Protection System devices for your Facility/Facilities.

· Reference Section G for different ways/forms that evidence of coordination may be provided (Attachment 1, 2, 3, etc.).

· The coordination must be verified at a maximum of every five calendar years.

PRC-024-2 Guidance and Expectations

· The Standard has a phased-in Implementation Plan.

· Per the Implementation Plan, 100% of applicable Facilities were to have the frequency and voltage protective relaying set per the Standard by July 1, 2019.

· New applicable Facilities must have the frequency and voltage protective relating set per the Standard by the time they are placed in service.

· R1 and R2 are applicable to the frequency and voltage protective relays applied on the individual generating unit of the dispersed power producing resources, as well as the frequency and voltage protective relays applied on equipment from the individual generating unit of the dispersed power producing resource up to the point of interconnection (reference Footnotes 2 and 4).

· For R2, note that the (voltage) protective relaying shall be set to not trip in the "no-trip zone" for voltage excursions **at the point of interconnection (POI)**. Reference the ERO endorsed Implementation Guidance "PRC-024-2 R2 Generator Frequency and Voltage Protective Relay Settings." This Implementation Guidance provides example calculations to validate compliance with PRC-024-2. In particular, the required relay element pickup voltage has to be reflected to the POI and account for the voltage drop across the GSU at the assumed loading level.

· Do not submit only relay setting sheets with the expectation that the auditor should determine if the relays are set per the Standard. Please provide evidence that your entity verified the relays are set per the Standard.

· It is recommended that the relay settings are displayed graphically on the curves in Attachments 1 and 2 of the Standard.

VAR-002-4.1 Guidance and Expectations

· Provide the voltage or Reactive Power schedule specified by the Transmission Operator. An auditor cannot determine if the voltage or Reactive Power schedule was maintained if the schedule is not provided.

· The auditor will use sampling to select generators and days when the generator was online and request evidence that the voltage schedule was maintained.

· If the voltage schedule was not maintained, provide evidence that the conditions of notification for deviations from the voltage or Reactive Power schedule were met and additional evidence showing the equipment was at its generating Facility's capabilities, if applicable.

· Evidence of the voltage every 10 minutes is generally acceptable.

· Graphical evidence (which displays the actual voltage, as well as the high and low voltage schedule limits) is recommended.

Overall Guidance and Expectations (For Any Standard)

· Strong internal controls will help ensure the desired outcomes of compliance and reliable operation. For help with Internal Control activities, please visit our Internal Controls Knowledge Center which provides guidance on analysis controls, second party reviews, contract (third-party) management, and documentation.

· If your entity has questions or needs help, please reach out to RF for assistance.

· The NERC website has guidance, implementation information, RSAW's, etc. by Standard and Requirement on its one-stop shop.

· Valuable information can be obtained by reading the RF bi-monthly newsletter articles; attending the bi-annual workshops, Internal Controls workshop and other subcommittee work/forums; listening in on the monthly reliability and compliance open forum compliance calls; and visiting the RF website to review the material in the Knowledge Centers.

· Use the RF Assist Visit Program. (Contact the RF Entity Development group for details.)

· If your entity concludes that there is a Potential NonCompliance (PNC), submit a self-report. It is better to self-report a PNC than to have the PNC identified during an Audit or Spot Check. Self-identification and working on the mitigation plan now will demonstrate that your detective controls are identifying issue(s) and your entity is constantly monitoring itself.

Winter 2019-2020

Reliability Resource Risk Assessment

The RF resource adequacy assessment for the upcoming 2019-2020 winter concludes that there should not be an issue supplying demand within the RF region. Both MISO and PJM are expected to have an adequate amount of resources to satisfy their respective planning reserve requirements. This seasonal assessment is based on data provided by PJM and MISO, and this article shares assessment highlights and statistics that support our analysis on outage risk.

PJM Capacity and Reserves

Net capacity Resources [1]	186,900 MW
Projected Peak Reserves	56,717 MW
Net Internal Demand (NID)	130,183 MW
Planning reserve margin	43.6%

The PJM forecast planning reserve margin of 43.6% is greater than the 16.0% margin requirement for the 2019 planning year. The planning reserve margin for this winter is higher than the 2018 forecast level of 40.0%. This is due to an increase in Net Capacity Resources when compared to the previous year.

MISO Capacity and Reserves

Net Capacity Resources	139,173 MW
Projected Peak Reserves	39,154 MW
Net Internal Demand (NID)	100,019 MW
Planning reserve margin	39.1%

The MISO forecast planning reserve margin of 39.1% is greater than their margin requirement of 16.8% for the 2019 planning year. The planning reserve margin for this winter is lower than the 2018 forecast level of 46.6%. This is mostly due to a decrease in Net Capacity Resources in MISO's footprint.

RF Footprint Resources

Net Capacity Resources	204,765 MW
Projected Peak Reserves	61,304 MW
Net Internal Demand (NID)	143,461 MW
Total Internal Demand (TID)	146,296 MW

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

Continued on page 13

Winter 2019-2020

Continued from page 12

Since both PJM and MISO are projected to have adequate resources to satisfy their respective forecasted planning reserve margin requirements, the RF region is projected to have sufficient resources for the 2019-2020 winter period.

Random Generator Outage Risk Analysis

This analysis evaluates the risk associated with random outages that may reduce the available capacity resources below the load obligations of PJM or MISO. Reports and/or other data released by PJM, MISO or NERC for this same period may differ from the data reported in this assessment due to different assumptions that were made by RF from the onset of the report.

This analysis differs from NERC's in that RF uses historical Generator Availability Data System (GADS) data from a rolling five-year period which provides a range of outages that occur during the winter period. The typical maintenance outages used in this analysis are derived from PJM and MISO for the winter months.

Exhibits 1 and 2 forecasted winter 2019-2020 demand and capacity resource data for the PJM and MISO RTOs. The daily operating reserve requirement for PJM and MISO at the time of the peak demand is also included as a load obligation.

The range of expected generator outages is included for typical maintenance and random outages. The random outages are based on actual NERC GADS outage data from December, January and February of 2014 through 2018.

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

The firm demand and the demand that can be contractually reduced as a Demand Response (DR) are shown in shades of green. The firm demand constitutes the Net Internal Demand (NID), with Total Internal Demand including the DR. The daily Operating Reserve requirement is shown in yellow between the NID and DR. With two different sets of demand bars, the chart shows both the 50/50 and the 90/10 demand forecasts.

For instance, the 50/50 demand forecast projects a 50% likelihood that demand exceeds 130,183 MW. The 90/10 demand forecast is a more conservative model, projecting a 10% chance that demand exceeds 136,600 MW. DR is at the top of the Demand bar since in our analysis it is utilized first to reduce the load obligation when there is insufficient capacity. In the event that utilization of all DR is not sufficient to balance capacity with load obligations, system operators may first reduce operating reserves prior to interrupting firm load customers.

While scheduled outages during the winter season are generally minimal, the Outages bar reflects the amount of Typical Maintenance Outages in gray. The remainder of the Outage bar represents the entire range of random outages which occurred during the five-year reference period. Pink shows 100% of the random outages; rose shows less than 100% down to 10%; and red shows less than 10% down to 0.2%.

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

Continued on page 14

Winter 2019-2020

Continued from page 13

matter of convenience in describing the analysis results.

The probability percentages related to the amount of random outages that equal or exceed the amount of outages shown above that line on the Outage bar are along the left side of the range of outages. Moving downward on the bar represents an increasing amount of random outages, with a decreasing probability for the amount of random outages.

In the PJM chart, the random outages represented by the bar above the 100% point is 540 MW. This means that the probability of there being at least 540 MW of random generation outages is 100%. Similarly, at the 10% point, the outages represented by the bar above the 10% point is 22,570 MW (540 + 22,030 MW). There is a 10% probability that there will be at least 22,570 MW of outages. As shown by the probabilities and corresponding amounts of random outages, the distribution of random outages is not linear throughout the range of outages observed.

Exhibit 2 illustrates the same analysis for MISO. The top of the 50/50 demand obligation bar for MISO represents TID with operating reserves.

Exhibit 1 - 2019/2020 Winter PJM Resources Availability Risk Chart

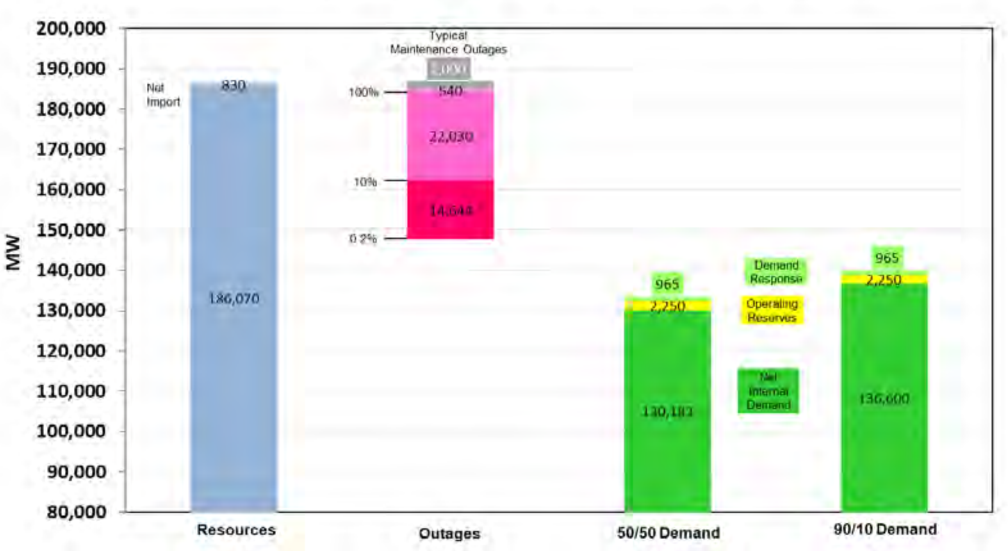
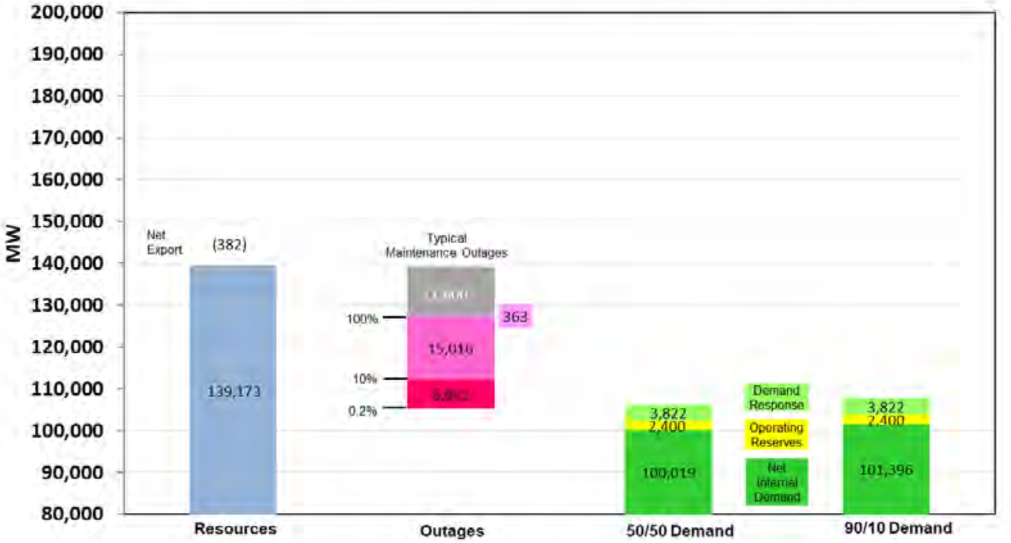


Exhibit 2 - 2019/2020 Winter MISO Resources Availability Risk Chart



The Lighthouse

By Lew Folkerth, Principal Reliability Consultant

Remote Access - Advanced Topics

In this recurring column, I explore various questions and concerns related to the NERC Critical Infrastructure Protection (CIP) Standards. I share my views and opinions with you, which are not binding. Rather, this information is intended to provoke discussion within your entity. It may also help you and your entity as you strive to improve your compliance posture and work toward continuous improvement in the reliability, security, resiliency and sustainability of your CIP compliance programs. There are times that I also may discuss areas of the Standards that other entities may be struggling with and share my ideas to overcome their known issues. As with lighthouses, I can't steer your ship for you, but perhaps I can help shed light on the sometimes stormy waters of CIP compliance.

In the March/April 2015 Newsletter I explored the basics of Electronic Security Perimeters (ESPs) and remote access (see article here). In this column, I'll discuss some advanced topics regarding remote access, including ways you can improve your compliance and security postures. Since I've seen many entities experience compliance issues in this area, my recommendations will go beyond the minimum requirements of the Standards. I do this to encourage you to improve the security of your BES Cyber Systems and to provide your entity with a more robust means of demonstrating compliance. One way of looking at remote access is that any communications traffic crossing your ESP boundary is remote access. However, the CIP Standards provide specific definitions and corresponding requirements for various types of remote access. While looking at this topic, I'll include considerations for CIP-005-6, Electronic Security Perimeter(s), which will take effect in the U.S. on July 1, 2020. Also, I will include considerations for CIP-012-1, Communications between Control Centers, even though it has not yet received regulatory approval in the U.S. In discussing electronic access control, I'll assume you are using a firewall as your access control device, but the discussion applies to other forms of access control as well, such as a router and its access control list (ACL).

Remote Cyber Asset Capabilities

In any remote access scenario, the capability of the remote Cyber Asset is of critical importance. At the high and medium impact levels, the remote Cyber Asset is any device outside the ESP that communicates with a device inside the ESP. At the low impact level, the remote Cyber Asset is any device outside the asset containing low impact BES Cyber Systems that communicates with a device inside the asset.

Sturgeon Point Light Station, MI - Photo by Lew Folkerth

You must ensure, and be able to demonstrate to an audit team, that any remote Cyber Asset does not meet the definition of a BES Cyber Asset. In other words, the remote Cyber Asset cannot have a 15-minute impact on the reliable operation of the BES. If the remote Cyber Asset does have this capability, then it meets the definition of a BES Cyber Asset and must be included in a BES Cyber System at the appropriate impact level. The BES Cyber System must then be accorded the protections of CIP-003-8 through CIP-013-1, as applicable to its impact rating. This applies to all remote access at all impact levels, not just Interactive Remote Access.

In support of this stance, let's refer to the FERC order that remanded an Interpretation of CIP-002-4, Critical Cyber Asset Identification, in March of 2013 (see inset). That order clearly states FERC's concern over the capabilities of remote Cyber Assets. While this order applies to CIP-002-4, which never became enforceable, the principle carries forward into CIP-002-5.1, BES Cyber System Categorization.

I'll add an example to that provided in the inset: a transmission operator's laptop computer is capable of Interactive Remote Access to the operator's normal workstation, which is a console within the Control Center. This console is a BES Cyber Asset included in a high impact BES Cyber System. Once the remote access is established, the operator can access the console as if the

Continued on page 16

Continued from page 15

14. For example, a laptop computer connected to an EMS network through the Internet may be used to supervise, control, optimize, and manage generation and transmission systems, all of which are essential operations. However, the proposed interpretation of "essential" may leave certain cyber assets lacking the required CIP Reliability Standards protection that could, if compromised, affect the operation of associated Critical Assets even though the unprotected cyber assets are using similar access and exerting the same control as cyber assets that are deemed under the proposed interpretation to be "necessary or inherent to the operation of the Critical Asset." The proposed interpretation, in effect, would create a window into the EMS network that could be exploited.

[Order on Interpretation of Reliability Standard, Docket RD12-5-000, March 21, 2013, at P14]

operator were sitting at the console keyboard. This will grant the operator the same operating capability as the console, which includes the ability to control various elements of the BES in real time. The operator's laptop computer can therefore have a 15-minute impact on the BES, which makes the laptop computer a BES Cyber Asset.

Another concern is the ability of the remote Cyber Asset to access or store BES Cyber System Information (BCSI). BCSI must be protected and securely handled during storage, transit and use as required by CIP-011-1 R1, Information Protection. If the remote Cyber Asset has the ability to access BCSI, then such access must conform to your information protection program required by CIP-011-1 R1. If the remote Cyber Asset has the ability to store BCSI, then it must be designated as a storage location for BCSI, and access to it must be authorized and verified in accordance with CIP-004-6 R4, Personnel & Training.

Procedural vs. Technical Controls

CIP-005-6 requires technical controls for each Requirement and Part. It's a good idea to layer procedural controls on top of the technical controls. This will reinforce the concept that remote access to protected systems must obey strict rules. But you must not rely on the procedural controls alone. Your firewall rules must protect your networks from inadvertent and malicious use of remote access.

Remote Access Protocols

Let's take a closer look at what constitutes a remote access client. The language of the Interactive Remote Access definition says that Interactive Remote Access uses a remote access client but doesn't further define what a remote access client is. This isn't really a problem because there is no way to determine what software is being used to initiate the access from a remote Cyber Asset. The only indication we have is the communication protocol being used to access the system within the ESP.

Your audit team will look at your firewall ruleset to see if any communication protocols capable of interactive access are permitted from a location other than an Intermediate System.

Here are some common remote access clients and the protocols they use:

Remote Access Client	Protocol	Well-known Port(s)
Remote Desktop	Remote Desktop Protocol (RDP)	TCP/3389
Terminal Emulator	Telnet	TCP/23
Many free and commercial programs	Secure Shell (SSH)	TCP/22
Web browser	HTTP, HTTPS	TCP/80, TCP/443
FTP Client	File Transfer Protocol (FTP)	TCP/20, TCP/21
File explorer, etc.	SMB	TCP/445
File explorer, etc.	NFS	TCP/2049, UDP/2049
MIB Browser	SNMP	TCP/161, UDP/161
Unix r-commands	rlogin, rcp, rsh, etc.	TCP/513

CIP-005-6 R2 Part 2.1 requires all Interactive Remote Access to utilize an Intermediate System. In order to enforce this Requirement you will need technical controls that do one of the following:

- Ensure that all communication protocols that permit interactive access into the ESP originate only at an Intermediate System. The firewall ruleset (or router ACL) will provide your auditors with the evidence they need to determine compliance.

- If you permit a remote access communication protocol from a Cyber

Continued on page 17

Continued from page 16

Asset other than an Intermediate System, you must provide additional technical controls to ensure that interactive access is not permitted.

One of the protocols listed in the table above is Secure Shell (SSH). SSH has many capabilities and can present problems in demonstrating that your Intermediate Systems are not being bypassed. The SSH client, which communicates with the SSH protocol, is designed for interactive access. But the SSH protocol is also commonly used for system-to-system access.

Interactive and system-to-system access both use the same protocol, so your firewall can't tell the difference. Neither can your auditors. It is up to you to be able to demonstrate that a remote connection using the SSH protocol from a Cyber Asset other than an Intermediate System cannot be used for interactive access. I plan to discuss methods of doing this in a future article.

Demonstrating Compliance

CIP-005-6 R2 Parts 2.1-2.3 do not require you to implement Interactive Remote Access. If you choose not to permit Interactive Remote Access into your ESPs, then you do not need Intermediate Systems, multi-factor authentication, etc. But you must still be able to demonstrate that your technical controls do not permit interactive access. And, as discussed above, if you do implement Interactive Remote Access you must still show that your Intermediate Systems cannot be bypassed with an interactive-capable protocol. Since this topic is inextricably entwined with firewall rule management as a whole, I'll base my discussion on CIP-005-6 R1 Part 1.3.

Demonstrating compliance with CIP-005-6 R1 Part 1.3 begins with your change management program for firewall rules. Before a new rule is put into production, it should receive a rigorous review. To avoid common problems with the documentation of access control rules, and to ensure your security is as effective as possible, I strongly recommend going beyond the minimal requirements of the Standard.

Here are the items I recommend you consider and document for each rule:

- Nature of the remote device: What type of device is at the far end of this connection? Who owns it? How is its security managed?
- What port or port range will need to be permitted? Is the traffic inbound or outbound?
- What protocol will be used on this connection?
- What is the operational purpose of this traffic? What does it contribute to the reliable operation of the BES?
- What type of access does this rule permit?
  - Interactive Remote Access
  - ESP-to-ESP
  - System-to-system
  - Vendor remote access
    - If so, you must have a method to disable the access per CIP-005-6 R2 Part 2.5
  - Control Center to Control Center
    - Prepare for CIP-012-1 protections (e.g., encryption)
  - Other?
    - If so, what?
- When this rule is implemented, what capability will the remote device have?
  - Could it have a 15-minute impact on the BES?
    - If so, it must be identified as a BES Cyber Asset, included in a BES Cyber System, and protected.
  - Could it have access to BCSI?
    - If so, your information protection program must be applied.
    - If it will be able to store BCSI, it must be identified as a BCSI storage location and access controlled per CIP-004-6 R4.
- What changes to remote systems, companies, etc. might cause this rule to be modified or removed? You should have a method of monitoring for events that should trigger a re-evaluation of a rule.

When you have the information listed above, I recommend that you perform a risk assessment of the rule in the context of the operational purpose of the rule. Your risk assessment should answer these questions:

- Does the capability provided by this rule justify the risk this rule adds?
- Can this traffic be intercepted?
- Can this traffic be compromised?
- Is this traffic considered Interactive Remote Access? If so, is it through an Intermediate System?

And, once you have assessed the risk of a rule, what mitigations should you apply to minimize the risk the rule presents?

- Can the scope of the rule (e.g., port ranges, address ranges) be

Continued on page 18

Continued from page 17

reduced?
- Should this traffic be monitored? If so, how?
- Should this traffic cause an alert? If so, under what circumstances?
- Does this traffic need additional protections? If so, what is needed?

In order to keep this information up to date, I recommend that you periodically review the information and assessments listed above. This is not explicitly required by CIP-005-6 but is a good practice to minimize both your security risk and compliance risk by catching changes that might slip through your normal processes.

I also recommend that you monitor traffic crossing your ESP boundary to look for patterns of traffic that are new, unexpected, or vary from your normal patterns. There are several commercial and open source tools to help you do this.

On the topic of monitoring, I also recommend monitoring the content of Interactive Remote Access sessions. Monitoring remote sessions can provide assurance that the remote access is being used in accordance with the need for which it was granted. This may need to be implemented on the Intermediate System, since encryption is required up to the Intermediate System.

Remote Cyber Asset Security

Many of the Cyber Assets that remotely access devices within the ESP are not within the scope of the CIP Standards. Even though they are not in scope, I recommend that you consider implementing controls to reduce the security risk these Cyber Assets present. For example, a device engaged in Interactive Remote Access over a Virtual Private Network (VPN) should not permit other network traffic at the same time as VPN traffic. This is known as split tunneling and is a serious risk to the protected Cyber Asset being accessed.

Protections on the remote Cyber Asset should include:

- Prohibiting split tunneling;
- Ensuring no personal devices can be used for remote access;
- Managing access permissions on the device – ensuring administrative access is strictly controlled;
- Managing security patches for all software on the device;
- Hardening the device to reduce its attack surface;
- Ensuring no unauthorized software can be installed on the device;
- Storing the device in a secure location when not in use;
- Keeping anti-malware software and signatures up to date; and
- Enabling a host-level firewall on the device.

This is not an exhaustive list, but it might serve as a starting point in your consideration of this issue.

General Recommendations

In summary, CIP-005-6 requires that you tightly control all traffic crossing the ESP border. You should document all traffic so there is no question of what the traffic is for and why it is needed. Meeting minimum compliance Requirements in this area may not be enough. You may find it useful to go beyond minimum compliance to ensure you have the documentation to provide an audit team with reasonable assurance that you are meeting compliance for each Requirement.

Requests for Assistance

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

Feedback

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

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

Regulatory Affairs

FERC Details Cybersecurity Program Priorities

FERC made a presentation detailing its continuing efforts to address cybersecurity challenges facing the nation's energy infrastructure. The presentation details several organizational changes intended to better focus resources on quickly evolving cyber challenges. Chairman Neil Chatterjee also announced that the Commission's Office of Electric Reliability would be realigning its functions to establish one division focused exclusively on cybersecurity.

Drawing on the experience and knowledge of each of the relevant offices, a recent FERC staff presentation identified five areas where Commission staff will strategically and collectively focus efforts to address critical cybersecurity challenges.

The five focus areas are:

(1) Supply Chain/Insider Threat/Third-Party Authorized Access;

(2) Industry access to timely information on threats and vulnerabilities;

(3) Cloud/Managed Security Service Providers;

(4) Adequacy of security controls; and

(5) Internal network monitoring and detection.

FERC also announced intended outreach activities, including monitoring supply chain security implementation and the industry's adoption of new technologies and services to address cyber infrastructure implementation, maintenance and/or management. The Office of Energy Infrastructure Security will continue to build its outreach initiatives, including voluntary network architecture assessments, and the Office of Electric Reliability will continue to conduct and participate in audits.

FERC Releases Report on Enforcement

FERC's Office of Enforcement released their annual Report on Enforcement. The report summarizes all of the publicly available material that the office has engaged in throughout FY2019, including anonymous discussion of non-public material. The Division of Audits and Accounting discussed compliance alerts for some of the areas that they believe could use greater attention to help prevent noncompliance. The alerts included: Allocated Labor, Allowance for Funds Used During Construction, Formula Rate Matters, Transmission Rate Incentives, Open Access Transmission Tariffs, Data Reporting by ISO/RTO Market Participants, Natural Gas Accounting and Tariff Matters, Oil Pipelines, Nuclear Decommissioning Trust Funds, and Consolidation, and Untimely Filing of Commission Reports.

The Division of Analytics and Surveillance and the Division of Energy Market Oversight both describe their process for monitoring and analyzing markets, trends and potential manipulation. The Office of Enforcement has retained their previous enforcement priorities:

(1) fraud and market manipulation,

(2) serious violations of the Reliability Standards,

(3) anticompetitive conduct, and

(4) conduct that threatens transparency in regulated markets.

The report also breaks down the number of audits and auditing functions performed in FY2019, as well as the number of investigative subjects and reports performed.

NARUC Prioritizes Cybersecurity and Ties between State and Federal Regulators

The National Association of Regulatory Utility Commissioners (NARUC) elected the organization's next president, Brandon Presley, a Commissioner from the Mississippi Public Service Commission. Presley will serve as the NARUC president until the 2020 annual meeting. He wants to increase contact and familiarity between state regulators and FERC, or other pertinent federal regulatory bodies. He also has met with FERC representatives to ensure consistent training in cybersecurity. Presley acknowledged that states have policies that sometimes conflict with FERC, but that there are still ways they can work together and increase the dialogue between commissioners on the state and federal level.

Standards Update

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

General NERC Standards News

Impact of new Reliability and Security Technical Committee (RSTC) on Standards Process

At its Nov. 5 meeting, the NERC Board of Trustees approved the formation of the Reliability and Security Technical Committee (RSTC). This new committee will be formed by merging the Operating, Planning and Critical Infrastructure Committees. According to Howard Gugel, NERC Director of Engineering and Standards, this change will likely result in the Standards Committee now going to the RSTC for legal and technical support for Standard Authorization Requests (SARs) and potential revisions to the Standards creation process to account for the new committee.

Other Resources Posted

NERC has posted the following additional resources:

· The presentation and streaming webinar from the Oct. 11 webinar regarding the recently published NERC Reliability Guideline: Recommended Improvements to Interconnection Requirements for BPS-Connected Inverter-Based Resources;

· A slide presentation providing an overview of CIP-003-8, which FERC approved by letter order on July 31;

· The slide presentation and recording from the Nov. 12 Project 2019-01 – Modifications to TPL-007-3 webinar;

· The slide presentation and recording from the Nov. 8 Guideline for Distributed Energy Resources (DER) Modeling for Bulk Power System Planning Assessments webinar; and

· The slide presentation and recording from the Nov. 18 Project 2017-07 – Standards Alignment with Registration webinar.

Notable FERC Issuances

FERC issued no relevant Standards orders in October and November.

Notable NERC Filings

In November, NERC filed the following with FERC:

· The 2019 Frequency Response Annual Analysis report for the administration and support of Reliability Standard BAL-003-1.1 – Frequency Response and Frequency Bias Setting.

NERC's filings can be found here.

Standards Update

New Standards Projects

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

Project 2017-07 - Standards Alignment with Registration	**Initial Ballot and Non-Binding Poll Comment Period**	**12/02/19 - 12/12/19 10/29/19 - 12/12/19**
Project 2016-02 - Modifications to CIP Standards (CIP-002-6 Draft 4)	**Additional Ballot and Non-Binding Poll Comment Period**	**12/06/19 - 12/16/19 11/1/19 - 12/16/19**
Technical Rationale for Reliability Standards	**Join Ballot Pools Non-Binding Polls**	**11/4/19 - 12/3/19 12/9/19 - 12/18-19**
Comment Period Open for Draft Reliability Guideline – Special Reliability Assessment: Potential BPS Impacts Due to Severe Disruptions on the Natural Gas System	**Submit comments via email using the comment form.**	**11/4/19 - 12/18/19**

Recent and Upcoming Standards Enforcement Dates	
January 1, 2020	CIP-003-7 – Cyber Security – Security Management Controls; IRO-002- 6 – Reliability Coordination – Monitoring and Analysis; PRC-026-1 – Relay Performance During Stable Power Swings (Requirements 2-4); TPL-007-3 – Transmission System Planned Performance for Geomagnetic Disturbance Events (Requirements 5, 5.1, 5.2, 9, 9.1, and 9.2)
April 1, 2020	CIP-003-8 – Cyber Security – Security Management Controls
July 1, 2020	CIP-005-6 – Cyber Security – Electronic Security Perimeter(s); CIP-010-3 – Cyber Security – Configuration Change Management and Vulnerability Assessments; CIP-013-1 – Cyber Security – Supply Chain Risk Management PRC-002-2 – Disturbance Monitoring and Reporting Requirements (50% compliance for Requirements 2-4, 6-11)
October 1, 2020	PER-006-1 – Specific Training for Personnel ; PRC-027-1 – Coordination of Protection Systems for Performance during Faults
January 1, 2021	CIP-008-6 – Cyber Security – Incident Reporting and Response Planning; PRC-012-2 – Remedial Action Schemes
July 1, 2021	TPL-007-3 – Transmission System Planned Performance for Geomagnetic Disturbance Events (Requirements 11 and 12)
January 1, 2022	TPL-007-3- Transmission System Planned Performance for Geomagnetic Disturbance Events (Requirements 6, 6.1-6.4, 10, 10.1-10.4)
July 1, 2022	PRC-002-2 – Disturbance Monitoring and Reporting Requirements (100% compliance for Requirements 2-4, 6-11)
January 1, 2023	TPL-007-3 – Transmission System Planned Performance for Geomagnetic Disturbance Events (Requirements R3, R4, 4.1. 4.1.1–4.1.2, 4.2, 4.3, 4.3.1, R8, 8.1, 8.1.1–8.1.2, 8.3, 8.4, and 8.4.1)
January 1, 2024	TPL-007-3 – Transmission System Planned Performance for Geomagnetic Disturbance Events (Requirements R7, 7.1, 7.2, 7.3, 7.3.1–7.3.2, 7.4, 7.4.1–7.4.3, 7.5, and 7.5.1.)

These effective dates can be found here.

CIP Auditor Lindsey Mannion Gives Presentation at Women in Technology Conference

THE HIGH IMPACT OF MENTORSHIP & NETWORKING FOR WOMEN IN TECH
Lindsey Mannion, Critical Infrastructure Protection auditor
Lauren Zink, Security Awareness Manager

Cleveland's 2nd Annual WITcon (Women in Technology Conference) took place at the end of October, and RF's Lindsey Mannion shared her knowledge with attendees about the high impact of mentorship and networking for women in the tech industry. Lindsey joined RF in March of this year as a CIP Auditor, and her participation in WITcon is an excellent example of the thought leadership demonstrated by RF employees.

In a joint presentation with Lauren Zink, Security Awareness Manager at Oportun and Lindsey's former mentor, she highlighted the powerful combination of feedback and support from a mentor with topnotch networking skills. Lindsey's recommendations for how to approach these proactive efforts to set oneself up for career success were enhanced by the firsthand lessons she wove into the presentation.

WITcon is hosted by GetWITit, a nonprofit organization with the specific mission to address the declining pipeline of women in technology. The 2019 conference theme was The New Blueprint for Leadership, and the conference offered four different tracks to an audience of 400 women: Leadership & Career Development, Innovation, Advanced Technology and Entrepreneurship.

RF Hires Communications Manager

ReliabilityFirst is pleased to welcome Megan Baucco as the Manager of Communications and External Training. In this newly-created role, she will manage RF's external messaging, publications, social media accounts, branding efforts and more. In addition to developing and implementing communications and media strategies, Ms. Baucco will be involved in workshops and stakeholder outreach.

As the first dedicated Communications employee for the organization, she brings a combination of fresh ideas and strong fundamentals to RF. Ms. Baucco has in-depth marketing, communications and public relations experience across a variety of disciplines. Her background includes expertise in copywriting/editing, channel management, corporate communications, social media, strategic planning, brand reputation and event planning.

Prior to joining ReliabilityFirst, Ms. Baucco focused on external communications, marketing strategy and media relations at American Greetings. She graduated from Penn State University with a Bachelor of Arts degree in journalism with concentrations in both business and communication arts & sciences.

Ms. Baucco is a native Clevelander who stays busy outside the office volunteering with animal welfare organizations, cheering for the Cleveland Indians, and enjoying the outdoors by exploring the city's Metroparks.

Save the Date

Internal Controls Workshop

February 12, 2020

RF Officially Launches Cyber Resilience Assessment Tool

This innovative new tool is a voluntary self-assessment available exclusively for entities within the RF Region to evaluate and benchmark their cyber resilience posture, as well as measure effectiveness.

Why Use the Tool?

The tool characterizes the operational resilience of an entity’s BPS infrastructure in the presence of cyber attacks. It generates a tailored report identifying areas of improvement through deeper insights into components and processes that impact cyber resilience.

Want More Information?

Please Contact Us and choose Resilience from the dropdown list of Areas.

RF Salutes Employees for Veterans Day

The RF office celebrated Veterans Day with a luncheon in honor of all military personnel who served our country to protect our freedom – especially the veteran members of the RF team. In addition to coming together to show our gratitude, the lunch included presentations from Tony Freeman and Shawn Barrett, both Senior Analysts in the Risk Analysis and Mitigation department, and Ray Palmieri, Senior Vice President and Treasurer.

Tony, Master at Arms Petty Officer Second Class Expeditionary Warfare in the Navy, gave a presentation focused on bridging the gap between the perspective of daily life for military members and civilians. Some examples included photos of his current office and coworkers as compared to his “office” and “coworkers” when deployed in Kuwait, Iraq and Afghanistan.

Ray shared a few words about his time in the Navy, experiences working on submarines, and the development of the technology he used.

Left to Right Front Row: Kristie Purcell, Ray Palmieri, Larry Bugh, Shawn Barrett

Left to Right Back Row: Tony Freeman, Dwayne Fewless

Shawn, Sergeant First Class in the Michigan Army National Guard, shared highlights and photos of his 20-year career. This included active duty at Fort Campbell, KY; security at the 1996 Summer Olympics in Atlanta; and deployment to Anbar Province, Iraq. He also brought some of his decorations and uniform to show the group, which included his Bronze Star Medal, Meritorious Service Medal, Iraq Campaign Medal and Combat Infantry Badge.

Michigan Renewable Energy Installations Up 57% in 2018

Michigan's 2018 Distributed Generation and Legacy Net Metering Programs Report shows that the number of projects grew by 1,942 from 2017 to 2018. The number of customers participating in the program increased by more than 59%.

At the end of 2018, the total capacity of the installations was approximately 43,481 kilowatts (kW), which was an increase of 13,910 kW. Although that shows a 47% increase, legacy net metering projects remain a small portion of Michigan's total retail electricity sales at .0048%.

ReliabilityFirst Members

AEP ENERGY PARTNERS
AES NORTH AMERICA GENERATION
ALLEGHENY ELECTRIC COOPERATIVE, INC
AMERICAN ELECTRIC POWER SERVICE CORP
AMERICAN TRANSMISSION CO, LLC
APPALACHIAN POWER COMPANY
BUCKEYE POWER INC
CALPINE ENERGY SERVICES, LP
CITY OF VINELAND, NJ
CLOVERLAND ELECTRIC COOPERATIVE
CMS ENTERPRISES COMPANY
CONSUMERS ENERGY COMPANY
DARBY ENERGY, LLP
DATACAPABLE, INC
THE DAYTON POWER & LIGHT CO
DOMINION ENERGY, INC
DTE ELECTRIC
DUKE ENERGY SHARED SERVICES INC
DUQUESNE LIGHT COMPANY
DYNEGY, INC
EDISON MISSION MARKETING AND TRADING, INC.
EXELON CORPORATION
FIRSTENERGY SERVICES COMPANY
HAZELTON GENERATION LLC
HOOSIER ENERGY RURAL ELECTRIC COOPERATIVE, INC
ILLINOIS CITIZENS UTILITY BOARD
ILLINOIS MUNICIPAL ELECTRIC AGENCY
INDIANA MUNICIPAL POWER AGENCY
INDIANAPOLIS POWER & LIGHT COMPANY
INTERNATIONAL TRANSMISSION COMPANY

Forward Together RF ReliabilityFirst

LANSING BOARD OF WATER AND LIGHT
LINDEN VFT, LLC
MICHIGAN ELECTRIC TRANSMISSION CO, LLC
MICHIGAN PUBLIC POWER AGENCY
MIDCONTINENT INDEPENDENT SYSTEM OPERATOR, INC
MORGAN STANLEY CAPITAL GROUP, INC
NEPTUNE REGIONAL TRANSMISSION SYSTEM, LLC
NEXTERA ENERGY RESOURCES, LLC
NORTHERN INDIANA PUBLIC SERVICE COMPANY
OFFICE OF PEOPLE'S COUNSEL, DISTRICT OF COLUMBIA
OHIO POWER COMPANY
OHIO VALLEY ELECTRIC CORPORATION
OLD DOMINION ELECTRIC COOPERATIVE
PENNSYLVANIA OFFICE OF CONSUMER ADVOCATE
PJM INTERCONNECTION, LLC
PPL ELECTRIC UTILITIES CORPORATION
PROVEN COMPLIANCE SOLUTIONS, INC
PUBLIC SERVICE ENTERPRISE GROUP, INC
ROCKLAND ELECTRIC COMPANY
SOUTHERN MARYLAND ELECTRIC COOPERATIVE, INC
TALEN ENERGY
TENASKA, INC
TENNESSEE VALLEY AUTHORITY
UTILITY SERVICES, INC
VECTREN ENERGY DELIVERY OF INDIANA, INC
WABASH VALLEY POWER ASSOCIATION, INC
WISCONSIN ELECTRIC POWER COMPANY
WOLVERINE POWER SUPPLY COOPERATIVE, INC