Issue 1
2018 January/February

INSIDE THIS ISSUE

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

Web: www.rfirst.org
Follow us on

RELIABILITY FIRST

A Note from the President

Tim Gallagher, President and CEO

Dear Stakeholders:

The start of a new year is a time known for setting resolutions and putting plans into action. As much of our Region is spending time indoors surviving another cold snap, it is a fitting time to reflect, measure our previous efforts, and think strategically as we continue moving forward on our goals.

This issue has a planning theme, where we share highlights from our Strategic Plan and a Q&A with our newly elected Board Chairs as they consider the year ahead. We recap our Risk Communications Plan and include a thoughtful piece on planning projects from our Manager of Entity Development.

As a Regional Entity, a significant part of our planning involves understanding and aligning with the ERO and its goals and mission, which is apparent from the article sharing our Annual Compliance Monitoring Process. Accordingly, we also highlight a few of NERC's plans with thoughts from NERC's interim President and CEO on our In the Industry page.

This issue's Lighthouse offers practical advice for planning patch management mitigation and we continue executing on our plan to share more on data analytics, with another article on data visualization.

Finally, I draw your attention to an unplanned success on our Watt's Up page, as we recognize our Chief Innovation Manager for leading a project with RF staff that is now a chapter in a book recently published by the London School of Economics.

Stay warm, and continue measuring your efforts and planning so that we can all strategically move forward together!

Tim

From the Board

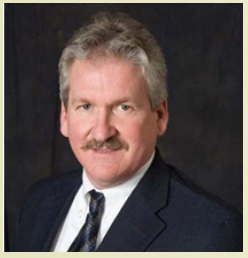
Introducing the 2018 Board of Directors

RF is pleased to introduce its 2018 Board of Directors. If RF members have questions for RF's Sector Directors, please feel free to contact the Director for your Sector. For all other inquiries, please contact Jason Blake, Vice President, General Counsel and Corporate Secretary. You can find more information on the Board of Directors here.

LISA BARTON
Chair
Supplier Sector
American Electric Power
Term Expires 2020

SIMON WHITELOCKE
Vice-Chair
At-Large
ITC Holdings Corporation
Term Expires 2018

MICHAEL BRYSON
RTO Sector
PJM
Term Expires 2018



KENNETH CAPPS
At-Large
Southern Maryland Electric Coop
Term Expires 2019

PATRICK CASS
Independent
Term Expires 2020

SCOTT ETNOYER
At-Large
Talen Energy
Term Expires 2020

BRENTON GREENE
Independent
Term Expires 2019

JAMES HANEY
Transmission Sector
FirstEnergy
Term Expires 2019

LARRY IRVING
Independent
Term Expires 2018

SUSAN IVEY
Large LSE Sector
Exelon
Term Expires 2019

MATT PAUL
Medium LSE Sector
DTE Energy
Term Expires 2019

LOU OBERSKI
Supplier Sector
Dominion Resources Services
Term Expires 2018

SUSAN SOSBE
Small LSE Sector
Wabash Valley Power
Term Expires 2020

LYNNAE WILSON
Transmission Sector
Vectren
Term Expires 2020

ReliabilityFirst
Board of Directors
and Committee Meetings
will be held at the RF
offices in Cleveland, OH on
March 14-15, 2018.

Click here for details

From the Board

Our new Board Chair Lisa Barton and Board Vice Chair Simon Whitelocke were both active members of our Board during the strategic planning process. We are very pleased to have them guiding RF and would like to share some of their thoughts on the new RF Strategic Plan for 2018-2022, and on the year ahead.

LISA BARTON
Chair

What role does the Board play when developing the Strategic Plan?

In November 2016, we began the process of seeking input. We started with the RF leadership team and stakeholders and had conversations with NERC Board members and senior executives and representatives from some of our sister Regions (SERC and WECC.) Then, through executive sessions with our leadership team, we considered all of the input and identified key issues.

What about the plan would you like to highlight?

As you would expect, the focus is on how to best achieve our mission of preserving and enhancing the reliability and security of the bulk power system in our footprint. The Strategic Plan focuses on four key strategic objectives to guide how RF performs its statutory activities:

1) Being a credible and informed regulator;

2) Making sound, risk-based decisions;

3) Deploying our resources effectively and cost-efficiently; and

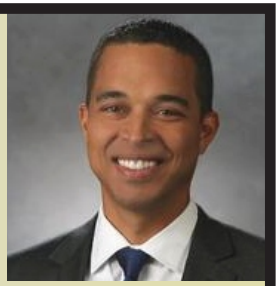
4) Serving as a transparent and collaborative leader.

Any final thoughts to share as you consider the year ahead?

As a Regional Entity, it is critical to ensure that we engage in the important task of strategic planning and focus on continuous improvement. Our expectations of our members is that they will consistently seek to improve their performance in the operations of the grid and we need to share that responsibility and commit to be adaptive to meet our compliance obligations.

What was the result of all those discussions?

The end product really is a collaborative effort that defines our priorities for the future and what we believe is a pragmatic and purposeful strategic plan. As always, we worked to ensure it aligns with and furthers the shared ERO Enterprise mission to ensure reliability and security across North America.



SIMON WHITELOCKE
Vice-Chair

Do you think the resulting plan was successful in positioning us for future success?

I am confident it will be successful in helping to propel RF forward in continuing to develop as a world class risk-based organization.

Any final thoughts to share as you consider the year ahead?

With significant changes and challenges expected in the generation resource mix, cyber and physical security, resilience and others, our strategic plan positions RF to adapt and prepare to meet our objectives.

RF Launches New Website

Our redesigned website offers quick and easy access to essential RF information and our activities. We will regularly update articles, upcoming events, and educational materials.

It is located at the same address: **https://rfirst.org**. Our new website is organized around four main categories, About Us, Program Areas, Knowledge Center and Committees. Each of these main topics has its own page with subpages, listed below. You will notice each of our departments has their own page to share content.

- LEADERSHIP
- BOARD OF DIRECTORS
- MEMBERSHIP
- TOOLS & PORTALS
- RF NEWSROOM
- UPCOMING EVENTS
- PUBLIC REPORTS
- CAREERS

- RISK ANALYSIS
  - COLD WEATHER PREPARDNESS
  - MISOPERATIONS
- WORKSHOPS
  - VIDEOS

- CIP LOW IMPACT FOCUS GROUP
- CRITICAL INFRASTRUCTURE PROTECTION COMMITTEE
  - RELIABILITY COMMITTEE
  - GENERATOR SUBCOMMITTEE
  - PROTECTION SUBCOMMITTEE
  - SPS REVIEW TEAM
  - TRANSMISSION PERFORMANCE SUBCOMMITTEE
- STANDARDS COMMITTEE

- COMPLIANCE MONITORING
- ENFORCEMENT
- ENTITY DEVELOPMENT
- EVENT ANALYSIS & SITUATIONAL AWARENESS (EASA)
- REGISTRATION & CERTIFICATION
- RELIABILITY ASSESSMENT & PERFORMANCE ANALYSIS (RAPA)
- RISK ANALYSIS & MITIGATION (RAM)
- STANDARDS

RF Launches New Website

Some areas we would like to highlight include:

NEWSROOM

- A Newsroom that features industry related articles and current news. You can access archived Newsletters and make sure you are subscribed.

UPCOMING EVENTS

- The Upcoming Events listing and tab has details on RF workshops, training, and meetings.

KNOWLEDGE CENTER

- The new Knowledge Center has educational materials on key topics related to reliability, security, and resiliency, and materials from RF Workshops and Webinar videos.

PUBLIC REPORTS

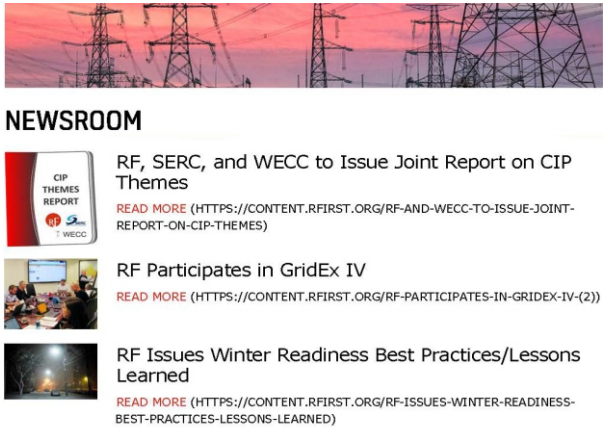
- Our Public Reports Page gives you access to RF Annual Reports and other reports on various topics.

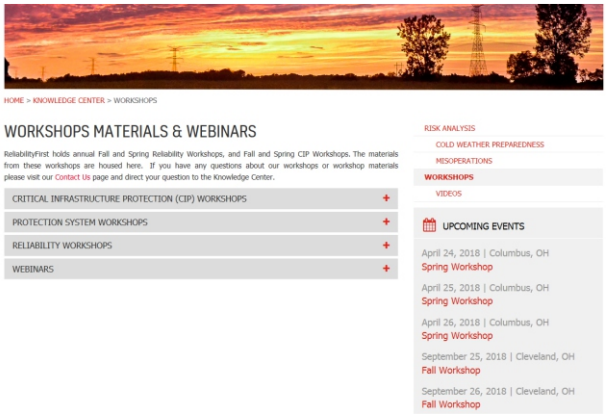
SEARCH FEATURE

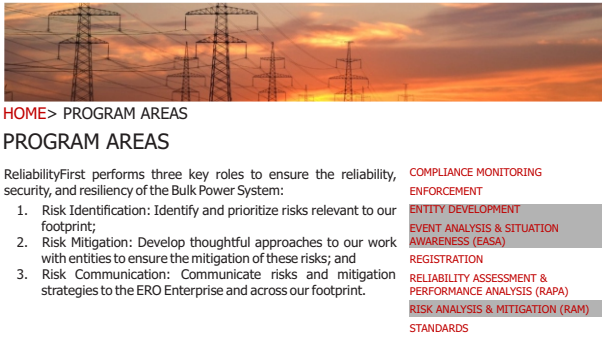
- If you don't see a specific document you are looking for you can always run a search that will pull up all related documents, presentations and articles regarding the topic you request. Then you can sort the results by category to narrow down a specific document type.

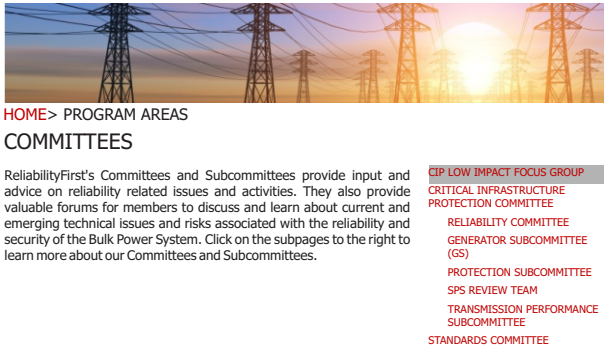
CONTACT US

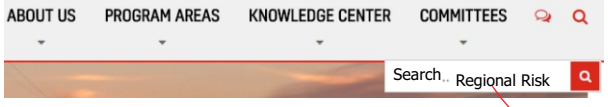
Please contact us with any questions, comments, or suggestions on the new website by visiting our "Contact Us" page.

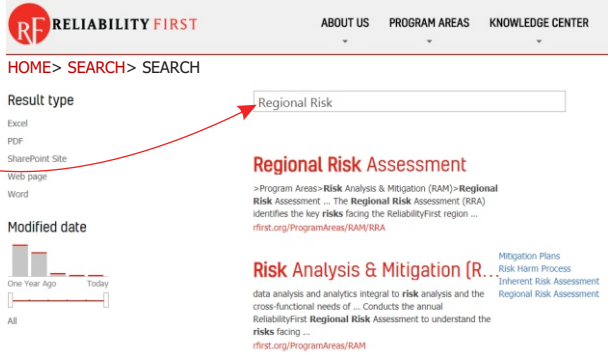












Project Planning

By: Erik Johnson, Manager Entity Development

You are a project planner. Even if you didn't realize it you plan projects all day long. Think of the last TV you purchased, or the Sunday evening week ahead plan you layout for your kid's activities, family activities, and the dreaded "other" category. Don't forget to factor in external interdependency impacts! The point is whether it's your intent or not, you do a lot of planning and it is often taken for granted and assumed to be "just part of what I do."

RF believes Ad hoc, or unplanned work, can produce unintended and undesirable consequences, thus creating risks to Bulk Electric System reliability and resilience. Additionally, unplanned work often results in cost and schedule overruns which, in turn, diminishes an organization's capacity to respond to threats to the bulk electric system's reliability and resilience.

The mechanism we use to identify strengths and weaknesses in entity project planning is the aptly titled Planning management practice. There are many steps along the journey of planning but the three high level objectives include:

1. Objective 1: Establish Estimates
2. Objective 2: Develop a Project Plan
3. Objective 3: Obtain Commitment to the Plan

Objective 1: Establish Estimates

Establishing estimates begins with the scope and impact of the project. Scope and impact analysis should be done to determine the needed resources, objectives and goals, risks assessments, and the length and relative difficulty of tasks and projects.

The scope and impact determinations are the building blocks for creating the project plan. Factors that affect scope include staffing, budgeting, and organizational or external requirements. When developing the initial scope of a project, soliciting input early from all stakeholders may eliminate risks that materialize later. This could include: Transmission Planning, Operations, Engineering Design, Maintenance, IT, Real Estate, Siting, Environmental Permitting, Project Management, Security, and Finance groups.

Scoping is also determined through project lifecycle management. A project lifecycle is a series of overlapping development phases, which creates opportunities for decision points.

- Decision points are used to reflect on the progress of the project and how well the project is mapping to the established goals, objectives, and constraints.
- Each decision point can result in new scope and impact determinations that affect the project plan.

Impact can be better assessed by breaking down large scale projects into logical components and then establishing estimates of work product and the associated effort to complete supporting tasks. Obtaining and tracking resources to implement a project can be burdensome, but is extremely important to project success.

- Is the work going to be performed with internal or external labor?
- Are there contracual obligations that must be met for internal resources?
- If external labor is selected, will the selected firm have resources available in the Winter, Spring, Summer, or Fall? Do available outage windows coordinate with the available resources?
- Do the possible resources have the experience and skillset to perform the required work?

Objective 2: Develop a Project Plan

The best method for protecting an organization from adverse effects on goals and objectives is to identify the risks and develop mitigating tasks; this is the basis of the project plan. Risks can impact various project attributes including scheduling, resource alignment and unity. A project plan keeps all the players on the same page. For the home and life decisions mentioned above, do you employ a shared family calendar? Or a big whiteboard that lists the weeks details? There you go planning again!

The mechanism an organization uses to identify risks can vary and may include performance models, brainstorming, expert elicitation, quantitative and qualitative risk assessments, and risk taxonomies. Once risks are identified, they should be considered for impact and probability of occurrence. Risks should also be prioritized based on potential harm to grid reliability and resiliency, factoring in the probability of occurrence.

Objective 3: Obtain Commitment to the Plan

A plan cannot be implemented without the commitment of those who are responsible for the output of the plan. In order to obtain commitment to the plan, the organization should review its plans, and determine which plans affect grid reliability so that key stakeholders are aware of the relationship among those plans. For example, plans that may require equipment outages (e.g., maintenance and testing programs) should be considered together to minimize impact on grid reliability. Commitment has to be achieved at a level of management that ensures resources and schedule attributes are met.

The commitment relationship must be managed, it is not a one and done but an ongoing relationship. The organization should embrace the iterative and adaptive process of reconciling work and resource levels rather than simply selecting levels at the outset and abiding by that original plan.

Conclusion

Planning is an important part of meeting project objectives. You plan even when you don't realize it. It is done in life tasks, as well as in work related projects. Since planning is such an integral part of our activities, we should not take it for granted and get better at it. I will leave it to you to think of all the arenas where results will improve due to sound planning.

Compliance Monitoring

Annual Planning Process

The ERO Enterprise Compliance Monitoring and Enforcement Program (CMEP) Implementation Plan (IP) is the annual operating plan that NERC and the Regions use to perform their CMEP responsibilities and duties. During the year, the CMEP IP is reviewed and may be updated on a quarterly basis. Updates may include, but are not limited to:

- Changes to compliance monitoring processes;
- Changes to Regional processes;
- Updates resulting from a major event,
- FERC directives
- Other matters (e.g., actions to address an emerging risk)

NERC posts any revisions to the CMEP IP on its website and issues an announcement to the industry.

RF's Appendix 4 to the CMEP IP provides:

- Details on RF's Regional Risk Assessment (RRA) processes and results;
- The Reliability Standards and Requirements associated with RF's RRA results;
- RF's Regional Compliance Monitoring Plan, which includes the annual audit plan; and
- Other key activities and processes used for CMEP implementation.

RF's Appendix 4 of the CMEP IP also provides information on the Risk-Based Approach to Compliance Monitoring and Enforcement. It discusses how RF customizes entities' oversight plans based on a number of considerations, including risk factors and registered entity management practices related to the detection, assessment, mitigation, and reporting of noncompliance.

It also discusses how RF focuses its enforcement resources on the higher risks to reliability, while maintaining visibility on lower risk issues.

Risk Elements and Associated Areas of Focus

This section of the CMEP IP describes how RF identifies risks and the mitigating factors that may reduce or eliminate a given risk. First, NERC identifies risk elements using data including: compliance findings; event analysis experience; data analysis; and the expert judgment of NERC and RE staff, committees, and subcommittees (e.g., NERC Reliability Issues Steering Committee (RISC)). NERC uses these risk elements to identify and prioritize interconnection and continent-wide risks to the reliability of the BPS. RF uses these risks, in addition to the risks specific to our footprint, to focus our monitoring activities and develop oversight plans for individual entities.

When developing entity-specific compliance oversight plans, RF considers local risks and specific circumstances associated with individual entities. The compliance oversight plan also takes into account the unique compliance history of each entity, and the timing and results of any prior compliance monitoring. The compliance oversight plan focuses on a complete picture of reliability risks associated with an entity along with various mitigating factors, such as past performance or the presence of effective internal controls.

A particular entity's scope of monitoring may include more, fewer, or different Reliability Standards than those outlined in the CMEP IP. The determination of the appropriate CMEP tools may be adjusted as needed within a given implementation year. Additionally, NERC and RF have the authority to monitor compliance with all applicable Reliability Standards regardless of whether they are identified as areas of focus in the CMEP IP or compliance oversight plan.

NERC Risk Element Results

The eight 2018 NERC risk elements remain unchanged from the previous two years. They are not a comprehensive list of all risks to the reliability of the BPS. Reliability Standards, Requirements, and associated functions for each area of focus may be updated throughout the year to reflect new versions of the Reliability Standards that become effective.

Areas of focus are provided for each of the risk elements. RF will consider the risk elements and areas of focus to help prioritize compliance monitoring efforts.

Table 1: Critical 2018 Risk Elements

2018 Risk Elements
Critical Infrastructure Protection
Extreme Physical Events
Maintenance and Management of BPS Assets
Monitoring and Situational Awareness
Protection System Failures
Event Response/Recovery
Planning and System Analysis
Human Performance

Regional Risk Assessments

RF performs a Regional Risk Assessment (RRA) to identify risks specific to our footprint that could potentially impact the reliability of the BPS. RF's Appendix 4 to the CMEP IP describes the Region-specific risks that result from the RRA. After determining Region-specific risks, RF identifies the related Reliability Standards and Requirements associated with those risks to focus monitoring activities. The identified risk elements serve as input when conducting an IRA and ultimately in determining the scope of an entity's compliance oversight plan.

Regional Compliance Monitoring Plan

RF provides a list of planned compliance monitoring activities for Compliance Audits, Spot Checks, Self-Certification, and Periodic Data Submittals. RF considers risk elements (both ERO-wide risk elements and RF risk elements), entity-specific risks, and other registered entity performance considerations and internal controls, to determine how RF will monitor an entity's compliance with Reliability Standards.

2018-2022 Strategic Plan

Click Here
To Learn More

ReliabilityFirst's 2018-2022 Strategic Plan (Strategic Plan) focuses on our mission of preserving and enhancing the reliability and security of the BPS in our footprint, and aligns with the shared ERO Enterprise mission to ensure reliability and security across North America.

The Strategic Plan focuses on the following four key strategic objectives to guide how we perform our statutory activities in support of this mission over the next five years:

Example Initiative:

Using information from system events, situational awareness tools, reliability studies, RTO studies, and other sources to help identify potential weaknesses/areas of focus for the Region

(1) Being a credible and informed regulator

- Have a deep understanding of our footprint and the risks we face
- Gather and assess data and information efficiently and effectively
- Continue to mature the ReliabilityFirst Regional Risk Assessment process, which focuses on the specific existing or emerging risks facing our footprint

Example Initiative:

Developing a risk register: a common repository for identified risks to help the organization in planning and conducting risk-based activities

(2) Making sound, risk-based decisions

- Understand and prioritize the risks we face
- Continually evaluate the effectiveness of our risk-based decision making

(3) Deploying our resources effectively and cost-efficiently

- Focus our activities in a manner that is commensurate with the significance of the risk posed to the bulk power system
- Share our expertise, and leverage the expertise of our entities, to advance industry practices surrounding risk identification, mitigation and prevention.

Example Initiative:

Leveraging the organization's external affairs function to communicate key risks and mitigation strategies in a compelling, targeted way across multiple communications channels

(4) Serving as a transparent and collaborative leader

- Act as a transparent and collaborative leader that values ideas and input from across the ERO Enterprise and our stakeholders
- Work with NERC and the other Regions to continuously improve our understanding of the bulk power system, our cost efficiencies, and the effectiveness of our activities.

Example Initiative:

Collaboratively developing cyber resiliency metrics to help guide the efforts of the organization, the ERO Enterprise, and the industry in this evolving area

Risk Communication Plan

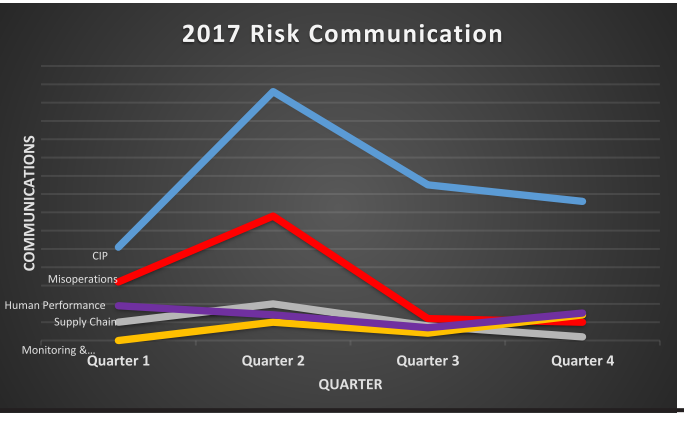
As a regulator tasked with preserving and enhancing electrical reliability, we strive not only to understand and mitigate risk, but also to effectively communicate it. RF prioritized the five risks to communicate in 2017.

To create our plan, we considered NERC's ERO Risk Elements and completed our Regional Risk Assessment. Then we evaluated those results and determined communication priorities based on criticality and our ability to maximize our impact over the year. We considered the existing knowledge level and capacity of our entities, their performance, and our own internal resources and expertise. We also took into account existing resources in the industry and across the ERO to ensure RF focuses its resources properly to enhance and fill knowledge gaps, without duplication.

Critical Infrastructure Protection (CIP)

Unsurprisingly, CIP has been a consistent priority across the ERO and our industry for years, and this continued in 2017. The cyber security landscape is inherently complex and as new threats and technologies evolve, entities see CIP as their greatest risk. Accordingly, RF appropriately directs much of its communication to assisting entities understand and mitigate these risks and ensure their compliance with the evolving suite of CIP Standards. Often, RF's efforts allow entities to go above and beyond compliance with the Standards.

In 2017, the consistency of our CIP communications continued with our reoccurring focus on CIP topics in each of our newsletters and a full day dedicated to CIP topics at our Fall and Spring workshops. Additionally, RF revisited previously identified themes in CIP compliance program deficiencies, and identified new trends within those themes. We communicated these CIP themes to entities at workshops and individually during enforcement engagements. Entity Development also performed assist visits to help individual entities evaluate and ensure robust CIP compliance programs. Our CIP communications this year emphasized physical security and entities with low impact assets (RF added a new focus group for entities with low impact assets). We also kept our CIPC and Board informed on relevant CIP topics throughout the year.



Protection System Failures (Misoperations)

RF decided to escalate its communications on Protection System Failures or misoperations in 2017, based on NERC's emphasis on lowering Misoperations rates across the ERO, and based on our diverse Region's performance in this area. Specifically, RF believes relay misoperations have the potential to be detrimental and it is important to define and quantify their impact on reliability in our footprint. We were confident we could have a measurable impact on this risk area, and the improved performance trend in our region has confirmed this. The peak communications outreach was a full day of our Spring Workshop dedicated to understanding and mitigating this risk, with presentations from internal and external experts. RF followed-up by continuing to ensure this content was communicated across our Region through our other vehicles (newsletter, compliance calls, social media.) RF undertook a targeted communications approach to mitigate this risk, by facilitating assist visits to help entities improve their performance.

Situational Awareness and Monitoring

Given the dynamic nature of the BES, operators may not make decisions that are appropriate for maintaining reliability without certain essential capabilities and up-to-date information that allow informed decision making. RF observed an increase of EMS-related events, and in addition to continuing to monitor and assist with mitigating them, decided to escalate its dedicated internal resources to this topic and increase communications. Due to NERC's existing EMS related resources and expertise, RF strategically paired with NERC on several efforts, including actively participating in the NERC EMS Working Group, presenting at the NERC Monitoring and Situational Awareness Conference, and taking a substantial role in the publication of the Risks and Mitigations for Losing EMS Functions Operating Committee Reference Document.

Supply Chain Management

Supply Chain Management was identified as an emerging risk that RF felt was worthwhile to focus on. RF has been closely following this risk, including serving on a panel at the Supply Chain Management Standard Technical Conference. RF continues to communicate with our entities on supply chain management issues, and is working to ensure entities are prepared for the new Standard as it approaches implementation.

Human Performance

Human Performance can have a widespread impact on reliability. Accordingly, RF increased our inclusion of this factor in our internal analyses and other risk communications. RF's Enforcement and Risk Analysis and Mitigation groups work closely with our entities to ensure that they identify and address the root cause or causes of each violation (which often involve human performance issues). In addition to working with entities during individual enforcement engagements, these groups have focused on targeted training to some of RF's larger entities to discuss best practices for developing mitigation to prevent recurrence of violations. Our goal is to ensure our Region remains aware of best practices and mitigation techniques and to continue to help them identify and mitigate risks, including those related to human performance.

Data Visualization

By: Kellie Anton, Senior Analyst-Data Analytics

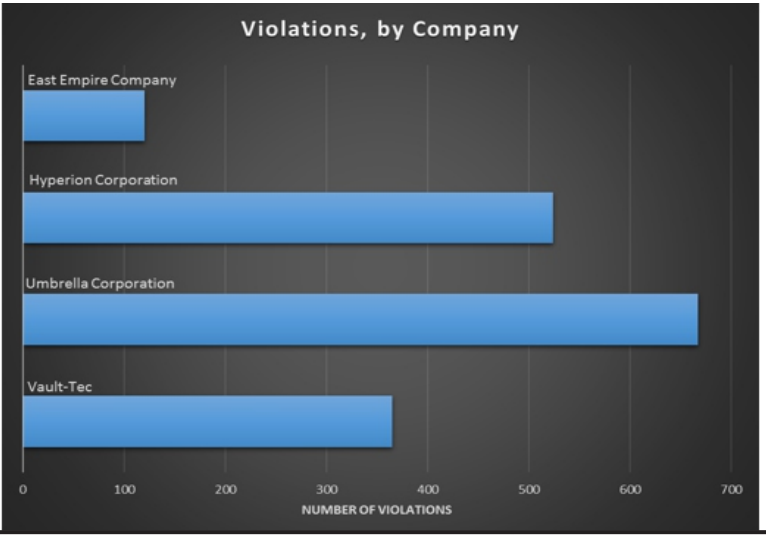
How to Make Effective Bar Graphs

For Data Analytics to be effective, communication is key and much of communication is in the visual design. To continue our series on data visualization, we will discuss the bar chart and highlight some potential design traps.

In the article on pie charts in our last newsletter, it was mentioned that humans generally have an easier time comprehending rectangles. It is easy for people to judge relative size, assess area, and quickly make conclusions based on the rectangular shape.

Bar charts offer a lot of flexibility as they can be presented in either a vertical (also known as column chart) or a horizontal format.

Choosing the correct format will depend on the information being communicated. Bar charts also allow for the display of negative numbers. Bar charts can be presented in a stacked format allowing comparison of part-to-whole relationships.



So, when should you use each type of bar chart? That will depend on the information which needs to be communicated.

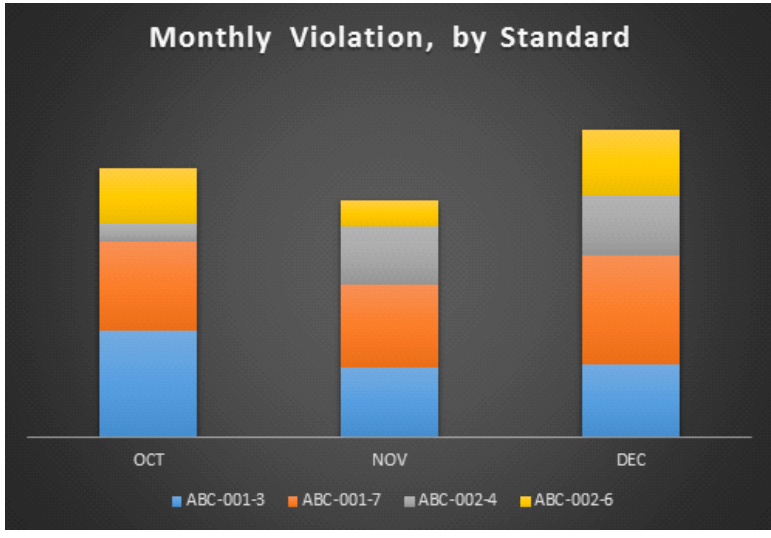
The horizontal bar chart (simply known as Bar in Excel) is great when charting different categories and when long labels are present in the information.

Notice how it is easy to read the information on number of violations for each company.

The vertical bar chart (simply known as Column in Excel) is also considered to be the standard bar chart. This particular type is really good for chronological data and when you have negative values in your data.

In discussing pie charts, it was mentioned that the same data could be presented as a bar chart. Stacked bar charts are great for showing that part-to-whole relationship and work best when presented as a 100% stacked bar. The stacked bar takes advantage of the ability to show the part-to-whole relationship over time which a pie chart cannot do.

Similar to the pie chart, the stacked bar chart should be limited to a small number of categories. Less than five is ideal, but up to six can be manageable. This can often be achieved by aggregating minor categories.



Continued on page 11

Data Visualization

Continued from page 10

There are few rules or best practices for designing your bar charts.

1. Start your y-axis at zero. Notice how December now appears to have more than twice as many violations? This provides a false assessment of magnitude.

2. Space the bars appropriately. The space between bars is far too large in this example. Try to keep the spacing between 50% and 100% of the bar width for optimal reading and space utilization.

3. Use consistent colors. Use one color for a bar chart. Multiple colors can lead to confusion and should only be used sparingly such as in a stacked bar chart. Also, consider monochromatic printing and color-blindness when choosing colors if multiple colors are appropriate.

When using bar charts, take the time to consider the information that is being presented, then use the bar chart format that best communicates the data story. Also, be wary of too much data or too many bars. A large number of bars will inevitably lead to a chart that is hard to read, as labeling becomes a challenge.

"7 Basic Rules for Making Charts and Graphs", FlowingData - click here;

"Bar Chart", The Data Visualization Catalogue, click here;

"Data Visualization: Chart Dos and Don'ts", Duke University Libraries, click here;

"How to Design Bar Charts", visage, click here.

MISO Board Approves MTEP17, $2.6 Billion Investment

Includes five interregional Targeted Market Efficiency Projects

The MISO Board of Directors in December approved 353 transmission projects – representing an investment of $2.6 billion – as part of the 2017 MISO Transmission Expansion Plan (MTEP17). The projects aim at improving energy access and reliability across the power grid.

The extensive upgrades included in MTEP17 ensure the continuing reliability of the regional grid, interconnect new generation supplies, provide for increased market efficiency, and reduce congestion between MISO and neighboring regions.

"These innovative, low-cost projects involve quick-implementation upgrades to reduce congestion across MISO-PJM seams," said Jennifer Curran, MISO's Vice President of System Planning and Seams Coordination.

"These projects can be accomplished with upgrades to existing equipment and offer positive value for customers."

The plan includes five interregional Targeted Market Efficiency Projects (TMEP) approved in partnership with the PJM Interconnection Board of Directors. TMEPs are designed to facilitate low-cost, high-value transmission projects to benefit customers and improve seams coordination with MISO's neighbors. The approved projects involve upgrades to existing facilities along the MISO-PJM seam in Illinois, Indiana, Michigan and Ohio.

The MISO Board also signaled their intent to approve in early 2018 an additional MTEP17 project – the Hartburg-Sabine Junction 500-kV Market Efficiency Project in Texas.

Once approved, the project will be eligible for MISO's competitive developer selection process. "MISO is pleased to recommend the Hartburg-Sabine project, as it will bring economic benefits to a transmission constrained area of Texas," noted Kent Fonvielle, Executive Director for the MISO South region.

MTEP is a robust, fully transparent planning process involving numerous discussions with MISO stakeholders across the footprint including MISO members, regulators, customers and neighboring systems. Since 2003, $15.4 billion of MTEP investments have been constructed across the MISO footprint, enhancing system reliability, reducing congestion, and enabling public policy requirements such as renewable portfolio standards.

"MISO's planning efforts are designed to develop transmission plans that offer customers reliable access to the lowest-cost electric energy through markets," Curran concluded. "We are pleased with this robust plan that supports those goals and also enables the interconnection of more than 5,000 megawatts of generation through new transmission assets."

The MTEP executive summary provides details about the projects and related analysis.

Enforcement Collaboration

By: Max Reisinger, Counsel and Matt Thomas, Manager CIP

Entity Self-Reporting & Upcoming Compliance Audits

Q What is an Entity supposed to do when it discovers a Self-Reportable issue after receiving the 90 Day Audit Notification?

A A Compliance Audit begins when an Entity receives the 90 Day Compliance Audit Notification. RF always encourages Entities to Self-Report issues as soon as possible upon discovery. This general rule holds true even when an Entity discovers the issue after receiving a 90 Day Audit Notification.

In this situation, the Entity should notify the Compliance Audit Team that it found an issue and that it will be Self-Reporting the issue. The Entity then should submit all relevant information in the Self-Report, including how the issue was discovered and why the entity is reporting it after receiving the 90 Day Audit Notification. Specifically, note in the Self-Report if the issue was discovered as result of an Entity's internal controls or if the issue was discovered during Audit related preparations or activities around the engagement (including questions raised from the Audit Team or in response to an Audit Team RFI).

This information included in the Self-Report should also be shared with the Compliance Audit Team. Fully disclosing the issue in the Self-Report to the Audit Team will allow the Audit Team to more completely and effectively evaluate an Entity's Compliance Program and assess the strength of the Entity's internal controls. Depending on the exact circumstances and time available, the Audit Team can also help an Entity develop and evaluate potential mitigating actions for the given issue or identify areas for improving an Entity's controls.

Q How will the Compliance Audit Team treat the Self-Report during the Compliance Audit?

A The table below summarizes how each circumstance will be addressed in the audit report, reporting prior to and after the 90 Day Audit Notification letter was issued. As a general rule, if the Compliance Audit Teams finds a noncompliance after issuing the 90 Day Audit Notification, even if that issue has been Self-Reported by the Entity, the Audit Team will write that noncompliance as a Potential Noncompliance (PNC). The Audit Team may also ask questions pertaining to an entity's internal controls and request additional information on an entity's mitigation of any noncompliance it finds during the Compliance Audit, including any Self-Reports.

At the conclusion of the engagement, all noncompliances and existing Self-Reports will be handed off to Enforcement for processing. If you have any questions about Compliance Audits, please feel free to reach out to Matt Thomas (Manager, CIP Compliance Monitoring) or Gary Campbell (Manager, Operations & Planning Monitoring). If you have any questions about the Enforcement Process, please reach out to your Case Manager.

Discovery Method		Audit Report Finding
Self-Report **prior to** 90 days		OEA
Self-Report **during** 90 days	If **discovered** by Audit Team (as a result of sampling, or additional evidence request made by the audit team where the audit team would have made a PNC determination and the entity submits a self-report)	PNC
	If **Entity identifies** (an issue through audit preparation that is outside of sample/scope of audit)	OEA

The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

Patch Management Mitigation Plans

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.

Q I have several BES Cyber Assets that cannot be patched. Is it possible to have a patch management mitigation plan in place that does not need to be updated with every patch that is released for these systems?

A CIP-007-6 R2 (Security Patch Management) requires a new or revised patch management mitigation plan for each and every applicable security patch that is not applied within the time window specified. Note that there are two types of mitigation plans that may apply to the CIP Standards (see sidebar, "Two Types of Mitigation Plan"). In this article, I will review how mitigation plans fit into a vulnerability management program and what the expectations are for those mitigation plans. I will also discuss some methods that might be used to make a mitigation plan easier to adapt to new vulnerabilities.

Two Types of Mitigation Plan

The "mitigation plan" (not capitalized) referenced by CIP-007-6 R2 should not be confused with the term "Mitigation Plan" (capitalized) defined in the NERC Rules of Procedure. As used in this article, "mitigation plan" refers to a plan used to mitigate a vulnerability, not a Plan to correct and prevent re-occurrence of a violation.

Vulnerability Management

In a vulnerability management program, a mitigation plan fills the security gap between the identification of a vulnerability and the vulnerability's removal from an affected system. A vulnerability is removed by modifying the software containing the vulnerability.

For more information about vulnerability management programs, see The Lighthouse in the July/August 2016 issue of the RF Newsletter.

This is usually done by applying a security patch, but may also be accomplished by upgrading to a version of software that does not contain the vulnerability or by removing the vulnerable software from the affected system. In any case, if the vulnerability cannot be removed in a timely manner it must be mitigated by a series of actions contained in a mitigation plan.

CIP-007-6 R2 addresses only those vulnerabilities that enter your vulnerability management program by way of the release of a security patch, but in my opinion you will best serve the needs of reliability by identifying all vulnerabilities that may impact your systems. Whether you implement a full vulnerability management program or stick with a basic patch management program, one of your primary sources for vulnerability identification will be security patches.

Eagle River, MI - Photo: L. Folkerth

CIP-007-6 R2 requires you to evaluate each security patch for applicability and within 35 calendar days of this evaluation apply the patch, create a new mitigation plan, or modify an existing mitigation plan.

Lifecycle of a Patch Management Mitigation Plan

A mitigation plan has several stages in its existence:

Creation – A mitigation plan is created in response to the release of a security patch that can't be applied within 35 days of the evaluation of the patch for applicability. The mitigation plan must include planned actions and a timeline.

Modification – This stage of the mitigation plan is optional. If the mitigating actions required for a newly released patch are similar to those of a previously mitigated patch, you may want to modify an existing mitigation plan rather than start a new one from scratch.

Mitigation Plan Approval – If a mitigation plan is modified, the modifications must be approved by the CIP Senior Manager or specified delegate. It would be prudent, although not required by CIP-007-6, for management to also review, assess, and approve new mitigation plans.

Continued on page 15

Continued from page 14

Execution – After a mitigation plan is created, the plan is executed to implement the mitigating actions specified by the plan.

Revision and Approval – If the mitigating actions are not completed by the dates specified in the plan's timeline, a new timeline must be developed and approved by the CIP Senior Manager or a specified delegate. Be aware that multiple extensions or a substantial extension of the timeline may be closely scrutinized by your audit team. You should carefully document the reasons for any timeline changes.

Completion – When all of the mitigation plan's mitigating actions have been performed, the mitigation plan is considered complete.

Maintenance – Once the mitigation plan is complete, ensure that any configuration items or other mitigating actions are not undone by subsequent changes. One way to accomplish this is to periodically monitor any configuration items that were changed by the mitigating actions. Changes to these configuration items need to be reviewed to verify they did not weaken the mitigations.

Termination – Vulnerabilities may be removed from applicable systems by several methods:

- patching the vulnerable software;
- upgrading the software to a version that does not have the vulnerability;
- uninstalling the vulnerable software; or
- decommissioning the Cyber Asset that contains the vulnerable software.

After all vulnerabilities covered by the mitigation plan are removed from all applicable systems, then the mitigation plan may be terminated and maintenance of the plan may cease. Remember to keep all of your documentation of the mitigation plan's implementation as audit evidence.

Expectations of a Patch Management Mitigation Plan

For the purposes of CIP-007-6 R2, I suggest a mitigation plan structure that consists of eight parts:

1. Identification of the vulnerability or vulnerabilities addressed.

   The mitigation plan should begin by listing the vulnerabilities it applies to. This can be accomplished by listing the patch that fixes the vulnerability, or by providing the National Vulnerability Database (NVD) identifier. Be aware that the NVD usually contains a Common Vulnerability Scoring System (CVSS) Severity Score that can be helpful in determining the overall risk presented by a vulnerability. This can be useful when assessing risk, as described in part 3 below.

2. Identification of the systems or types of systems affected.

   At a minimum, you should record the in-scope systems that have this vulnerability. You will want a control in place to ensure that vulnerable systems are not missed. An automated tool can assist here.

   As a part of your list of affected in-scope Cyber Assets it may be useful to keep the patch status of each system and the date patched. This ensures all information about the vulnerability is in the same place.

3. Consideration of the methods that might be used to exploit the vulnerability.

   This is where you begin developing your mitigating actions. Identify the means an attacker might use to take advantage of the vulnerability in your networks. By considering how a vulnerability could be exploited, you will also identify the risks to your systems. Documentation of these risks can be used in other phases of the mitigation plan to help in establishing prioritization, timing, resource allocation, etc.

4. Mitigating actions to prevent the exploits from occurring.

   From your analysis of the possible attack vectors in step 3, develop a list of configuration items to change and other actions you will take to protect your affected systems. Note that these protections need not be the same for each system, but may reflect different levels of risk based on the location of the system, the function of the system, and other factors.

5. Action items to implement.

   Develop action items and document how you will implement the mitigating actions. Each action item should be a discrete task that can be identified and tracked.

6. Target dates for each action item.

   Assign completion targets for each action item or task. These target dates should reflect the risk posed by the vulnerability and the possible exploits. High risk items should receive immediate attention. Lower risk items can be scheduled when resources are

Continued on page 16

Continued from page 15

available. While CIP-007-6 R2 doesn't specify a timeframe for implementation of the mitigation actions, you must be able to demonstrate to an audit team that your implementation dates are prudent. In my opinion, a good guideline to use would be to mitigate high risk vulnerabilities within a couple weeks of discovery, while it might be reasonable to allow very low risk items to go as long as three months. Whatever approach you take, be sure you document your risk-based approach to determining target dates.

7. Monitoring steps.

   You should maintain a list of configuration items that will be monitored to ensure the mitigating actions remain in effect until the vulnerability is removed from all target systems.

8. Conditions upon which the mitigation plan may be terminated.

   You should list the patches that need to be applied in order for the mitigation plan to be terminated. If a software upgrade is expected to remove the vulnerability, list the minimum version of the software that is required. Or, if it will take a complete system replacement to remove the vulnerability, that should be stated. This information will enable you to determine when the mitigation plan may be terminated (see Lifecycle above).

Note that if you employ an automated patch management system, you may be able to extract much of the required information from that system.

Improving the Coverage of an Existing Patch Management Mitigation Plan

The actions I propose above for a mitigation plan involve a substantial amount of work. If you are in the situation where you are not able to patch systems within the 35-day window, then you will need to become very efficient at developing, implementing, and monitoring mitigation plans. This may include patching delays of:

- Several weeks (e.g., the systems are in a transmission substation and you can't touch them during peak load season),
- Several months (e.g., you need a generating plant scheduled outage of several days to be able to patch), or
- Several years (e.g., a previous patch can't be applied because it interferes with the functioning of the system and subsequent patches are cumulative, so you need a "fork-lift" upgrade to fix the vulnerability).

One way of becoming more efficient might be to categorize mitigation plans by the type of vulnerability addressed. For example, your mitigation plans for Microsoft Server Message Block (SMB) vulnerabilities may contain similar actions. If you already have a mitigation plan that addresses SMB vulnerabilities, it might be easier to modify that plan rather than start a new one from scratch. It is possible you may only need to update the applicable patches and reconsider the possible attack vectors.

Keep in mind that even if you don't need to take any additional mitigating actions because the ones you have in place are effective against exploits of the new vulnerability, you still must revise the mitigation plan. The plan needs to reflect the new patches and any new vulnerabilities identified, even if the mitigating actions are the same.

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.

Feedback

Please share any feedback you may have on these articles. Suggestions for topics are always appreciated. I may be reached here.

FERC Requests Comments on Resilence

In the same Order that FERC used to reject the DOE's NOPR to subsidize coal and nuclear plants, FERC requested that regional grid operators (RTOs/ISOs) review a comprehensive list of questions about the current state of the grid within 60 days. FERC wants regional grid operators to detail how they could enhance grid resilience.

Specifically, FERC asked for more information on how pricing reforms in PJM and ISO-New England can impact resilience. After the regional grid operators' comment, industry participants will have 30 days to reply to those comments.

FERC plans on using the responses from regional operators and industry participants to holistically examine the resilience of the BPS, to evaluate how RTOs/ISOs assess threats to resilience, and to evaluate options to mitigate threats to resilience.

In their first public appearance after FERC rejected the DOE's NOPR, Commissioners Chatterjee and LaFleur agreed that Secretary of Energy Rick Perry raised legitimate issues about grid resilience in the NOPR, but proposed the wrong remedy for those issues. Both Chatterjee and LaFleur confirmed that FERC would not favor certain fuel sources and that FERC will take a fuel-neutral approach in its resilience docket.

FERC Unanimously Rejects DOE Proposal

In January, FERC rejected the Department of Energy's Notice of Proposed Rulemaking (NOPR) to subsidize coal and nuclear plants. The five-member Commission unanimously rejected the proposal.

The NOPR, which the DOE presented to FERC in September of 2017, would have provided short-term cost recovery for power plants that retain 90 days of fuel onsite (i.e., coal and nuclear plants) in order to keep the baseload plants online and operating. The DOE filed a new version of the proposal in October of 2017, which stated that the cost recovery would only apply to merchant plants in Independent System Operator (ISO) and Regional Transmission Operator (RTO) jurisdictions with "energy and capacity markets."

The plants mentioned in the proposal are at risk of retirement as renewable energy and natural gas plants have provided cheaper ways to generate power with fewer carbon dioxide emissions. DOE Secretary Rick Perry argued that coal and nuclear resources are vital to the BPS because they are more resilient in extreme weather conditions, specifically citing the Polar Vortex in 2014 as an example. Opponents of the NOPR argued that coal and nuclear resources are not any more resilient than natural gas and renewables and that almost all power outages are caused by something other than fuel supply issues.

FERC stated that the reasoning for rejecting the proposal is that the DOE's proposed rule did not fulfill the following requirements of the Federal Power Act:

1. The existing RTO/ISO tariffs are unjust, unreasonable, unduly discriminatory or preferential.
2. Any remedy proposed must be just, reasonable, and not unduly discriminatory.

In FERC's Order rejecting the DOE's proposal, FERC commended Secretary Perry for reinforcing the resilience of the BPS as an issue that warrants further attention. FERC, however, also noted that Perry's solution could have added billions per year to energy costs for ratepayers and the grid without appreciable improvements to reliability.

FERC also stated that it has already taken actions that address grid resiliency such as:

1. A multi-year effort to evaluate the coordination of wholesale natural gas and electricity market scheduling, resulting in significant improvements to those scheduling and coordinating processes.
2. An examination of the grid's response to events of the 2014 Polar Vortex and how each RTO/ISO addresses fuel assurance.
3. Approval of significant capacity market reforms in ISO New England and PJM designed to bolster performance from capacity resources to help address fuel supply issues during periods of system stress.
4. Working to address BPS reliability through new NERC CIP cybersecurity Standards that address physical threats and geomagnetic disturbances.

Neil Chatterjee, who served as FERC's Chairman from August to December 2017, authored a concurrence to FERC's Order. In that concurrence, he emphasized his belief that FERC's Order is a solid first step, but that interim measures may be needed to avoid near-term BPS resilience challenges from unprecedented changes in the generation resource mix.

FERC Commissioners Richard Glick and Cherly LaFleur also both authored concurrences. Glick stated that the DOE's proposal was insufficient and incorrectly aimed at subsidies rather than resilience. Cheryl LaFleur stated that the proposal was long on generalizations but short on evidence and disagreed with the DOE's emphasis on supporting coal and nuclear resources.

FERC Proposes Mandatory Expanded Cyber Security Incident Reporting

On December 21, 2017, FERC issued a Notice of Proposed Rulemaking (NOPR) to revise CIP Reliability Standard CIP-008-5, which addresses incident reporting and response planning. The Resilient Society filed a petition asking FERC to implement a new Reliability Standard for malware detection, removal and reporting. FERC declined the Resilient Society's recommendation, due to Standards and initiatives that already address this issue, but agreed that there should be broader incident reporting requirements. FERC stated its concurrence with NERC that the current reporting threshold for Cyber Security Incidents may not reflect the true scope of cyber-related threats facing the BPS.

In the NOPR, FERC proposes modifying the CIP Standards to include mandatory reporting of Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's Electronic Security Perimeter (ESP) or associated Electronic Access Control or Monitoring Systems (EACMS).

FERC also proposes modifying the CIP Standards to specify the information that must be included in each Cyber Security Incident report. This would include (1) the functional impact, when identifiable, that the Cyber Security Incident achieved or attempted to achieve; (2) the attack vector used to achieve or attempted to achieve the Cyber Security Incident; and (3) the level of intrusion achieved or attempted.

Finally, FERC proposes modifying the CIP Standards to establish a deadline for filing a report once a compromise or disruption to bulk electric system operation, or an attempted compromise or disruption, is identified by a responsible entity. The reports submitted under the enhanced mandatory reporting requirements would be provided to the Electricity Information Sharing and Analysis Center (E-ISAC), and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), similar to the current reporting scheme.

In the Industry

NERC Interim CEO Charlie Berardesco Discusses ERO Enterprise Long Term Strategy

The ERO Enterprise undertook a number of strategic initiatives to enhance efficiency and effectiveness in 2017, including the first ERO Enterprise Long-Term Strategy, which identifies significant new developments and related risks affecting reliability, and establishes key focus areas to guide the ERO Enterprise's work over a five-to-seven year horizon.

"The plan provides an excellent basis on which to develop the ERO Enterprise's coordinated annual budgets and business plans and three-year work plans, enabling everyone to keep a laser-like focus on achieving the ERO's mission," said Charles A. Berardesco, interim president and chief executive officer of NERC.

"Going forward, NERC remains focused on its core mission to assure reliability and security of the bulk power system, as well as remaining agile in order to identify and address dynamic challenges."

NERC Approves ERO Enterprise Strategic Plan and 2018 Metrics

On November 17, 2017 the NERC Board approved the 2018 ERO Enterprise Strategic Plan and metrics. Both are created with input from stakeholders, the Reliability Issues Steering Committee, the NERC Board of Trustees and Regional Entity Boards.

The Plan details the contributing activities for five identified goals and outlines metrics focused on measuring progress on reliability improvement. Each goal is connected to associated metrics, and the contributing activities are mapped.

The goals of the Plan are:

- risk-responsive Reliability Standards;
- objective and risk-informed compliance monitoring, enforcement, and organization certification and registration;
- identification and mitigation of significant risks to reliability;
- identification and assessment of emerging risks to reliability; and
- effective and efficient ERO Enterprise operations.

NERC Board Approves ERO Enterprise Long-Term Strategy

During its February meeting, the NERC Board approved the ERO Enterprise Long-Term Strategy, discussed resilience and accepted a special assessment.

The Long-Term Strategy looks ahead five-to-seven years to review how changes in the industry will affect the ERO Enterprise. It highlights emerging and potential reliability impacts and incorporates recommendations from the Reliability Issues Steering Committee's draft report.

Board Chair Roy Thilly discussed resilience and the need to look at the various components of resilience and build upon them. He noted that there is a strong consensus that resiliency is already built into NERC's efforts. The Board requested the RISC to review how NERC's mission currently incorporates resilience of the BES.

The Board also approved NERC's Special Assessment: Potential Bulk Power System Impacts Due to Severe Disruptions on the Natural Gas System, which analyzes potential reliability impacts of natural gas disruptions.

The assessment finds that the impacts from natural gas facility disruptions vary depending on the location and infrastructure density, and those mitigation strategies can reduce potential impacts. To learn more click here.

Standards Update

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

General NERC Standards News

NERC Webinar Resources for Standards Changes

FERC issued Order No. 836, approving Balancing Authority Control (BAL-005-2) and Facility Interconnection Requirements (FAC-001-3). These will become effective on Jan. 1, 2019. This Order also retires Inadvertent Interchange (BAL-006-2) at the end of this year. NERC slide presentations discussing these changes are available here along with webinar here: 836 Order

FERC issued Order No. 837, approving Remedial Action Schemes (PR-012-2), that becomes effective January 1, 2021. A NERC slide presentation discussing these changes is available here, along with a webinar link here: 837 Order

Standards Efficiency Review Project

NERC's Standards Efficiency Review Project page has been added to the Initiatives dropdown on the top navigation bar of NERC's website for easy access. The Standards Efficiency Review evaluates NERC Reliability Standards using a risk-based approach to identify potential efficiencies through retirement or modification of Reliability Standard Requirements.

Notable NERC Filings

In December, NERC filed the following:

- the 2018–2020 Reliability Standards Development Plan informational filing, consisting of a status update on active development projects, a forecast of future work to be undertaken by industry participants and NERC throughout the upcoming year, and an analysis comparing completed projects and development accomplishments with the prior year's plan.
- comments in response to the notice of proposed rulemaking proposing to approve proposed Reliability Standard CIP-003-7 – Cyber Security – Security Management Controls.

NERC filings to FERC can be found here, organized by year.

New Standards Projects

Projects are described on the NERC Standards website, along with links to all drafts, voting results, and similar materials. Recent additions include:

Posted for Comment

- Project 2017-05 – NUC-001-3 Periodic Review | Preliminary Team Recommendation; Comment Period; 12/15/17 – 01/29/18

More information on this and other balloting and commenting events is available here.

Other Active Comment Periods

- NERC Seeks Industry Input for Standards Efficiency Review; Submit the completed spreadsheet to Chris Larson;12/13/17 – 02/02/18

New Entity Profile Questionnaire Tool

RF is rolling out a new Entity Profile Questionnaire tool to collect data and information to evaluate and understand the potential impact that your Entity may have on the Bulk Electric System. RF plans to use this information to perform its Compliance Monitoring and Enforcement Program activities more effectively and efficiently.

The focus of the collection will be based on your Entity's organizational makeup, technical information, compliance history, culture, overall Entity performance, industry trends, and numerous attributes and qualities of your compliance program.

RF plans to roll this tool out to all of its Entities in 2018.

- To do so, RF will send requests out to Entities in groups of approximately 40 about every two months.
- RF will use MKInsight to facilitate this collection.

Coupled with the roll out, RF will be conducting informational/training webinars.

- The webinar will focus on the purpose, training and next steps of the new Entity Profile Questionnaire tool.
- Preceding each informational/training webinar (for a batch of Entities), a Doodle poll will be circulated to request availability for each training session.

If you have any questions or concerns, you can contact RF at entityprofile@rfirst.org.

Standards Update

Recent and Upcoming Standards Enforcement Dates

April 1, 2018

- IRO-018-1 Reliability Coordinator Real-time Reliability Monitoring and Analysis Capabilities
- TOP-010-1 Real-time Reliability Monitoring and Analysis Capabilities

July 1, 2018

- CIP-009-6 Cyber Security Recovery Plans for BES Cyber Systems (Requirement 2.3)
- CIP-010-2 Cyber Security Configuration Change Management and Vulnerability Assessments (Requirements 3.2, 3.2.1, 3.2.2)
- MOD-026-1 Verification of Models and Data for Generator Excitation Control System or Plant Volt/Var Control Functions (Requirements R2, 2.12.1.6)
- MOD-027-1 Verification of Models and Data for Turbine/Governor and Load Control or Active Power/Frequency Control Functions (Requirements R2, 2.1-2.1.5)
- TOP-001-4 Transmission Operations
- TPL-007-1 Transmission System Planned Performance for Geomagnetic Disturbance Events (Requirement 2)

September 1, 2018

- CIP-003-6 Cyber Security Security Management Controls (Requirement 2, Att. 1, Sec. 2 and 3);

January 1, 2019

- BAL-005-1 Balancing Authority Control
- FAC-001-3 Facility Interconnection Requirements
- TPL-007-1 Transmission System Planned Performance for Geomagnetic Disturbance Events (Requirement 5)

January 1, 2020

- PRC-026-1 Relay Performance During Stable Power Swings (Requirements 2-4)

July 1, 2020

- PRC-002-2 Disturbance Monitoring and Reporting Requirements (50% compliance for Requirements 2-4, 6-11)

January 1, 2021

- PRC-012-2 Remedial Action Schemes
- TPL-007-1 Transmission System Planned Performance for Geomagnetic Disturbance Events (Requirement 6, 6.1-6.4)

January 1, 2022

- TPL-007-1 Transmission System Planned Performance for Geomagnetic Disturbance Events (Requirements 3,4,7)

July 1, 2022

- PRC-002-2 Disturbance Monitoring and Reporting Requirements (Requirements 2-4, 6-11)
- VAR-501-WECC-3 – Power System Stabilizer (Requirement 3 has an effective date of July 1, 2022 for units placed in service prior to final regulatory approval.)

More information on these and other upcoming Standards is available here.

Watt's Up at RF

RF Training Plan

Planning is essential to ensure the diverse training needs within our organization are met and executed in a way that strengthens our organization. Last month, our staff spent some time focusing on interpersonal skills, projects, and collaboration tailored to improve our core work.

Each staff member was assigned to one of twelve distinct teams based on their role, responsibilities and DiSC styles. Throughout the dedicated days our entire staff worked collaboratively in cross-functional teams to achieve results.

Highlights included:

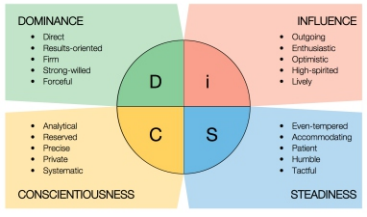
(1) a project management simulation that challenged staff to identify issues and deliver better results to maximize business value while balancing the diverse needs of our stakeholders;

(2) analyzing personality styles with Motivators assessments, that explored seven distinct areas that explain what matters to each employee's inherent needs and values and drives their performance;

(3) examining our approach to being adaptable and how to best present messages of change; and

(4) concentrating on Writing to Inform and Writing to Influence and how to hone and present a message or story in the most effective way.

While the January training was on interpersonal skills, projects, and collaboration, several additional trainings are planned throughout the year to address the needs of our diverse departments and staff.



Carl Dister has been with RF since 2011, and has over 30 years of experience in systems engineering.

RF Research Published in London School of Economics Handbook

RF is pleased to announce that a project led by Carl Dister, Chief Innovation Manager, has been published in the London School of Economics (LSE) Handbook of Research Methods in Complexity Science.

Inspired by NERC's Reliability Assurance Initiative in 2012, Carl began researching various methods around the world that aid in analyzing the reliability of complex systems like the grid. The resulting RF research is now one of the 26 chapters in the Handbook, alongside others by various academic researchers and practitioners in the field of complexity science around the world. Also called systems theory, complexity science merges social science with physics and the use of big data methods to resolve problems within complex systems. The book provides in-depth case studies meant to provide concrete examples of complexity science in everyday life scenarios, including organizations, infrastructures, higher education institutes, and music performance.

Q How did RF become involved with this project?

A During a comprehensive search for methods in analyzing reliability, a particular roadmap caught our attention. It turned out the author was a researcher right in Ohio, specifically Brian Castellani, a sociology professor at Kent State University's Ashtabula campus. Brian had created an interactive global complexity science roadmap that displayed applied research in complex systems over the last 100 years. The LSE was interested in putting a case study in their handbook that utilized the SACS toolkit, an intermediary instrument with an algorithm for researchers to model complex systems with web data. Brian Castellani is the main developer of the toolkit, and it had only been applied to the fields of public health and psychology. RF was interested in utilizing the toolkit for infrastructure, which we worked on, and the LSE selected it for inclusion in the Handbook.

Q Tell us about your chapter in the book.

A Our work is featured in Chapter 14: Modeling Social Complexity in Infrastructures: A Case-based Approach to Improving Reliability and Resiliency. Along with another professor at Kent's Ashtabula campus, Dr. Rajeev Rajaram, Brian Castellani and I used the SACS toolkit method to investigate the root causes of reliability issues within the grid. I noticed that misoperations was a key risk in our region, and we had yet to make much headway in finding its root causes. From a systems theory perspective, it appeared that the root causes of the problem may go beyond the equipment itself. Considering rates for crime, physical and mental illnesses, unemployment, and other social factors both in our country and in our communities we can get an idea of other issues that may cause power industry workers, both in the field and in the office, to make mistakes at work.

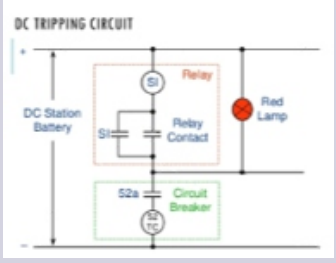
Q What impact do you think the work could have on electric reliability?

A I think it can challenge us to dig a little deeper when we look at the causes of certain events. Perhaps we could get to a point where we really evaluate the underpinning of human behavior in the workforce. Already, we are beginning to address Human Performance as a risk to the grid, with NERC hosting their Human Performance Conference last year and RF hosting one this year. We have identified that human behavior can cause problems, but we have yet to fully understand and address all the ways this can translate to potential risks to the grid. We are doing this more as we continue our use of management practices, which drive improved performance by focusing on human beings. Finally, the fact the book is out of London may help encourage the consideration of international perspectives and challenge us to think globally to address complex issues on our bulk electric system.

Watt's Up at RF

Protection System Workshop
August 14-15, 2018
Cleveland, OH

The RF Reliability Assessment and Performance Analysis (RAPA) group is hosting its third annual protection system workshop for technical personnel. This workshop will focus on Protection System Drawings – the Big Picture.



Intended Audience (This is not a compliance related event)

- **Substation designers, drafters, electricians, supervisors, field engineers**
- **Relay technicians, engineers and others who work directly with this equipment**
- **Company trainers on this subject**

Should you have any questions on these two workshops, please contact John Idzior or Jeff Mitchell.

Human Performance Workshop
August 15-16, 2018
Cleveland, OH

RF is hosting a human performance workshop for technical personnel. This workshop will focus on practical application of human performance techniques and concepts for front-line activities that attendees can take back and use in transmission reliability related work areas such as operations, asset management, design, protection, maintenance, and others.

Intended Audience: those with a focus on front-line activities in reliability related work areas.

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

RF Spring Workshop

April 24-26, 2018

Nationwide Hotel and Conference Center
Lewis Center, OH
(Columbus Area)

Day one is the Reliability Workshop, and the primary focus will be on Situational Awareness and EMS outages. This workshop will help you better recognize and understand the causes, trends, and internal controls around EMS outages. It will also help you to mitigate risks associated with the loss of situational awareness within your organization.

Day two is the Compliance User Group (CUG) meeting. Additionally, the Critical Infrastructure Protection Committee (CIPC) group (invite only) will meet during the afternoon.

Day three is the CIP Workshop, with topics that address cyber standards, issues, and practices that affect security.

Save the Date

Follow RF on LinkedIn

@RFirst_Corp

Calendar of Events

Complete calendar of RF Upcoming Events is located on our Website:

Date	RF Upcoming Events	Location
Feb 19	Reliability and Compliance Open Forum Call	Conference Call
Mar 14	Board of Directors and Committee Meetings	Cleveland, OH
Mar 15	Board of Directors Meeting	Cleveland, OH
Mar 19	Reliability and Compliance Open Forum Call	Conference Call
Apr 16	Reliability and Compliance Open Forum Call	Conference Call
Apr 24-26	RF Spring Reliability Workshop and CIP Workshop	Columbus, OH
Apr 25	ReliabilityFirst CIPC Meeting	Columbus, OH

Industry Events:

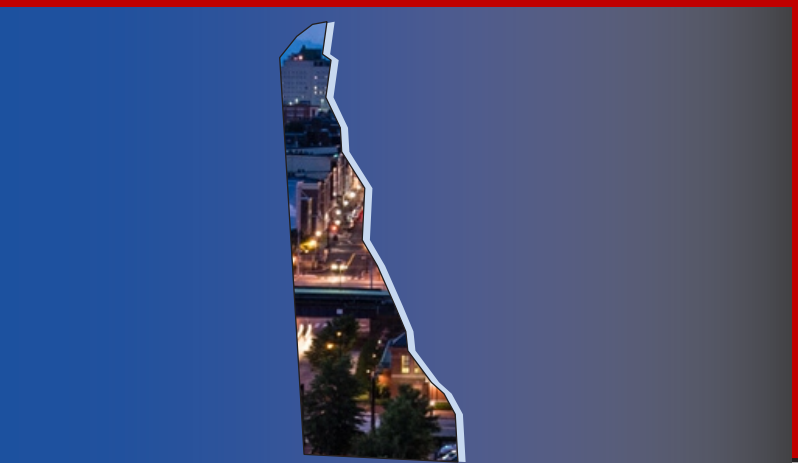
Date	Industry Upcoming Events
Feb 15	FERC Open Meeting
Feb 27	NERC Webinar - Risk & Mitigations for Losing EMS Functions
Mar 1-2	NERC GADS Wind Training
Mar 07	NERC Emerging Technology Roundtable
Mar 15	FERC Open Meeting
Mar 26-29	NERC Human Performance Conference and Workshops
Apr 19	FERC Open Meeting

SHARE YOUR FEEDBACK

Please email any ideas or suggestions for the newsletter to prcommrequest@rfirst.org

SUBSCRIBE TO THE NEWSLETTER

Click Here



Delaware Ranked #10 in Grid Modernization

Delaware was ranked 10th in the United States for the degree in which states are moving toward a modernized grid.

The report by Gridwise Alliance noted that Delaware posted a strong showing in Grid Operations (#8) and solid performance in State Support (#17). A strong suit for Delaware is transportation electrification, where the state incentivizes homeowners and businesses to install electric vehicle charging stations. The University of Delaware continues to develop and deploy vehicle-to-grid technology designed to leverage these installations.

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 ENERGY RESOURCE MANAGEMENT CO
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

Forward Together RF ReliabilityFirst

INTERNATIONAL TRANSMISSION COMPANY
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