Issue 4
2018 July/August

INSIDE THIS ISSUE

ReliabilityFirst Corporation
3 Summit Park Dive, 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,

We tailored this issue to address some of the risks and challenges faced by smaller entities in our footprint. RF has a diverse footprint with over 230 Registered Entities. These include Regional Transmission Organizations and formerly integrated utilities with generation, transmission and distribution assets. But many more entities are generator owner/operators or distribution providers.

By smaller, we don't mean simply geographic size because we are also considering resources, roles and responsibilities, and overall impact to the BPS. All of these entities play a role in preserving and enhancing the reliability and security of the grid. Our smaller entities are vital and valuable contributors to reliability and have been outstanding partners since our inception, from serving on our Board, helping us test risk based concepts, and contributing in our many stakeholder forums and committees.

We know smaller entities face unique challenges—from resource constraints to having their staff wear multiple hats—and with the transition to a risk-based enterprise, it may feel like our engagements focus on larger entities. We wanted to take this opportunity to ensure we are speaking to our smaller entities.

Therefore, this issue includes resources and advice on topics we thought would be pertinent to our small entities and serve as reminders for things they may not encounter as frequently as some of our larger entities.

Some highlights in this issue include: information and reminders on audits; event analysis and the importance of internal controls; a lighthouse tailored to CIP issues for smaller entities; and some lessons learned from NIPSCO.

Beyond this issue, remember we have lots of resources available on our website, or as always we encourage you to reach out to our Entity Development group.

ReliabilityFirst is here to help as we are all in this together. Our success is very much tied to the success of all of our members, big and small.

Forward Together,

Tim

From the Board

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

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

I serve as the Senior Director for Talen Energy's NERC & Cyber Protection program, which includes nineteen NERC-registered plants across the United States. I have worked in the electric generation industry for more than twenty-five years, including various management positions in operations, project management, corrective actions programs, emergency planning, and regulatory compliance. I have also served in the FERC Office of Electric Reliability, where I supported Reliability Standards development.

Additionally, I was the founding Chairman for what is now known as the North American Generator Forum, and received certification as a Senior Reactor Operator while working at the Calvert Cliffs Nuclear Plant. I am a veteran of the U.S. Navy, having served as a Machinist Mate on board the USS Hyman G. Rickover, a nuclear-powered submarine stationed out of Norfolk, Virginia. I earned a B.S. in Nuclear Engineering Technology from Thomas Edison State College and an MBA from Pennsylvania State University.

What sparked your interest in joining the RF Board?

I was excited to join RF's Board because of their strong engagement with stakeholders and sincere commitment to reliability. RF does everything with excellence. The high-quality work throughout the organization allows them to produce high quality results, which is something I am proud to be a part of. This dedication to quality and continuous improvement also makes RF a leader in the ERO.

How did you think your background will contribute to serving RF?

In my industry, the way we do business is unique. We work with very real financial constraints, and we have a real commitment to efficiency. With limited resources, efficiency and accuracy are just how we operate. It is cheaper to do it right the first time than it is to go back and correct a mistake. I believe I will bring that point of view and that commitment to the Board.

What is happening in the industry today that you are most excited about?

When RF sees concerns they reach out and proactively address them. I think that mindset is starting to spread whether it is with fuel resiliency or other evolving areas. There are efforts being taken across the ERO to understand risks and address areas of improvement. In the end, security matters--reliability matters. We have to protect our industry. What we do here matters, and I am pleased to see RF and the industry taking that seriously.

Are you involved in any other activities outside of work?

Two years ago, I hesitantly began Young Life's mentorship program. I wasn't sure what I, as an educated adult male in the electric industry, had to give to at-risk adolescents, but it has been one of the most rewarding opportunities I have experienced.

We asked Ken Capps from our Board, a current At-Large Director and former Chair (2013-2015), to share some thoughts for this issue on both representing the small entity perspective on our board and how RF can assist small entities.

"RF has always taken steps to make sure that everyone necessary for ensuring reliability has a seat at the table. As the Senior Vice President and Chief Operating Officer for Southern Maryland Electric Cooperative, Inc. (SMECO), I've personally helped ensure small entity perspectives are represented on the Board since 2005.

As a small customer-owned electric cooperative serving as an At-Large Director, I bring the understanding of working with tight margins while also prioritizing responsive, reliable, and resourceful power.

In my role at SMECO, I've also seen the benefit of some of RF's initiatives firsthand, and how engagements like assist visits can be tailored to small entities and help get a holistic look at their operations to see where value can be added under tight constraints."

SMECO
Southern Maryland Electric Cooperative

Great Things Come In Small Packages

By: Carl Dister, Chief Innovation Manager

The Power Industry is not unique in considering the impact of "Small Entities." In the past several decades, industries developing and operating complex, life-critical equipment developed a set of controls based upon their lessons learned and best practices.

In 1969, these were released as a US Military Standard, then later adopted by the international community and the IEEE as ISO/IEC/IEEE standard 15288. (15288, 2002)

With the globalization of the 1990's, it was apparent that a "one size fits all" international standard like ISO/IEC/IEEE 15288 would not work for small enterprises. The international community came together and decided that it was critical to profile these standards for enterprises with 25 employees or less. However, even with 25 employees, the need to have solid controls was critical, although a set not as extensive as those that exist in a larger enterprise could be considered.

You may think, at first glance, why the bother? After all, for a large aircraft, or a large piece of medical equipment, what impact could such a small enterprise of 25 people have? It turns out for highly complex sociotechnical systems, like aircraft systems and medical devices, even the smallest subsystem could potentially have a high impact.

Many people in the Power Industry will quickly recognize this as a "black swan" or high impact, low probability event. So, how do you make sure these small enterprises can still make a profit, but at the same time, prevent negative impact upon the entire system? Through profiles.

International Systems and Software developers have adopted a global profiling standard: ISO/IEC 29110: Systems and Software Life Cycle Profiles and Guidelines for Very Small Entities. The INCOSE Very Small Entity Working Group helps companies to understand how to adopt this standard in practice.

Here is the purpose of this ISO/IEC 29110 standard – it should resonate with all small entities offering reliable electric service:

> *"Very Small Entities (VSEs) around the world are creating valuable products and services. For the purpose of ISO/IEC 29110, a Very Small Entity (VSE) is an enterprise, an organization, a department or a project having up to 25 people... It has been found that VSEs find it difficult to relate International Standards to their business needs and to justify the effort required to apply standards to their business practices.*
>
> *Most VSEs can neither afford the resources, in terms of number of employees, expertise, budget and time, nor do they see a net benefit in establishing over-complex systems or software lifecycle processes...To address some of these difficulties, a set of guides has been developed based on a set of VSE characteristics. The guides are based on subsets of appropriate standards processes, activities, tasks, and outcomes, referred to as Profiles.*
>
> *The purpose of a profile is to define a subset of International Standards relevant to the VSEs' context"*
> *(International_Standards_Organization, 2015)*

For example, for the basic profile of one small

Today, several industries adopt these high-level controls, including Aerospace, Transportation, Medical, Manufacturing, and the US-UK-European Military. These controls contain subsets of preventative, detective, and corrective controls organized into these high-level processes:

- Acquisition Process
- Supply Process
- Enterprise Environment Management Process
- Investment Management Process
- System Life Cycle Processes Management Process
- Resource Management Process
- Quality Management Process
- Project Planning Process
- Project Assessment Process
- Work productivity assessment measure
- Product quality assessment measures
- Project review
- Project Control Process
- Decision Making Process
- Risk Management Process
- Information Management Process
- Stakeholder Requirements Process
- Requirements Analysis Process
- Architectural Design Process
- Implementation Process
- Integration Process
- Verification Process
- Transition Process
- Validation Process
- Operation Process
- Maintenance Process
- Disposal Process

Continued on page 4

Great Things Come In Small Packages

Continued from page 3

system service provider, the ISO/IEC 29110 suggests this subset of controls found in the ISO/IEC/IEEE 15288 document:

- System Requirements Engineering
- System Architecture
- Interface Management
- System Integration, Verification, and Validation
- Configuration Management
- Project Management
- System Deployment

Here is another small entity profile example. A small Canadian transportation company applied ISO/IEC 29110 to their services. After profiling, the company found that they matched with CMMI-DEV (SEI, 2010) level 2 controls (Laporte, Tremblay, Menaceur, Poliquin, & Houde, 2016). The table to the right from the CMMI-DEV lists the high-level internal controls suggested as a company moves up from a lower Maturity Level to a higher one. Notice how many fewer Level 2 controls there is then the list above for the entire ISO/IEC 15288 list.

In the Power Industry, VSE's could start the profiling process by listing the services they deliver, the risks they pose to the grid, and the value they bring during resiliency efforts. Then, RF's Entity Development group can help them with the optimum selection of controls for their profile.

For help finding the right set of controls for your business, contact Erik Johnson in the Entity Development group at ReliabilityFirst for an assist visit today!

References

15288, I. I. (2002). System Life Cycle Process: ISO Geneva,, Switzerland.

International_Standards_Organization. (2015). Systems engineering — Management and engineering guide: Generic profile group: Entry profile *ISO/IEC TR 29110-5-6-1:2015(en)* (Vol. Systems and software engineering — Lifecycle profiles for Very Small Entities (VSEs) — Part 5-6-1): ISO/IEC.

Laporte, C. Y., Tremblay, N., Menaceur, J., Poliquin, D., & Houde, R. (2016). *Developing and implementing systems engineering and project management processes at CSiT–A small Canadian company in public transportation.* Paper presented at the INCOSE International Symposium.

SEI, C. M. (2010). CMMI-DEV_V1_3. *Software Engineering Institute, 1.3*, 482.

Table 3.2 Process Areas, Categories, and Maturity Levels

Process Area	Category	Maturity Level
Causal Analysis and Resolution (CAR)	Support	5
Configuration Management (CM)	Support	2
Decision Analysis and Resolution (DAR)	Support	3
Integrated Project Management (IPM)	Project Management	3
Measurement and Analysis (MA)	Support	2
Organizational Process Definition (OPD)	Process Management	3
Organizational Process Focus (OPF)	Process Management	3
Organizational Performance Management (OPM)	Process Management	5
Organizational Process Performance (OPP)	Process Management	4
Organizational Training (OT)	Process Management	3
Product Integration (PI)	Engineering	3
Project Monitoring and Control (PMC)	Project Management	2
Project Planning (PP)	Project Management	2
Process and Product Quality Assurance (PPQA)	Support	2
Quantitative Project Management (QPM)	Project Management	4
Requirements Development (RD)	Engineering	3
Requirements Management (REQM)	Project Management	2
Risk Management (RSKM)	Project Management	3
Supplier Agreement Management (SAM)	Project Management	2
Technical Solution (TS)	Engineering	3
Validation (VAL)	Engineering	3
Verification (VER)	Engineering	3

Lessons Learned with CIP-010 Compliance

By: Mark D. Kelly, CIP Systems Specialist 2, NIPSCO and M. Bryan Little, Senior Counsel, NiSource Corporate Services

When NIPSCO Operations Technology (OT) first began the process of preparing for the new requirements in CIP Versions 5 and 6, our CIP-010 R1 baselines were developed and maintained manually in spreadsheets. NIPSCO quickly realized we were in need of a solution to replace this time consuming manual process.

To improve this process, NIPSCO OT developed a baseline process that is electronically managed using Tripwire Enterprise and the Whitelist Profiler application within Tripwire. This method has several benefits, including automated baseline comparisons, automated CIP-005 and CIP-007 security control testing, and evidence collection for changes to the baselines.

To begin the conversion process, Windows devices were the first baselines to be converted, followed shortly by baselines for Linux devices. As with any vendor solution, the challenge is converting the previously manually maintained records into Tripwire.

Network ports were the first area of focus when converting the baselines. Adding the network ports to the Whitelist Profiler configuration file allowed us to define what ports and associated processes were allowed to be present on the device as part of the baseline (CIP-010 R1.1.4).

We found that using the custom fields in the Whitelist Profiler allowed us to document business justifications and vendor documentation; this further demonstrates the need for the port (CIP-007 R1.1).

Installed software was also added to the Whitelist Profiler configuration file. Additional fields in the Whitelist Profiler were used to specify whether the installed software was commercially available, open-source, or custom software (CIP-010 R1.1.2 and R1.1.3). Software name and version are tracked as part of this process.

Operating system version (CIP-010 R1.1.1) and any applied security patches (CIP-010 R1.1.5) were tracked as part of custom Command Output Capture Rules (COCR) in Tripwire Enterprise. These are managed directly within the Tripwire Enterprise application as opposed to a configuration file for the Whitelist Profiler.

Once all of these CIP-010 baseline elements were added, we were able to automate the monitoring of the baseline (CIP-010 R2.1). For all baselines that were converted to Tripwire, the manual processes were reduced or eliminated, which led to reduced time and cost.

As part of maintaining baselines in Tripwire Enterprise, we were able to use reports from Tripwire as evidence for changes made to the baseline. Tripwire detects any changes to the baseline elements and those changes are then reviewed and promoted within the application. As part of the promotion process, the change ticket number is included as the approval ID (CIP-010 R1.2) in Tripwire Enterprise, which provides a reference to the change ticket that authorized the actual baseline change.

Date and time stamps of the detected change and corresponding promotion in Tripwire Enterprise provide strong evidence that the baseline was updated within 30 calendar days of completing the change (CIP-010 R1.3).

Test environment devices are also included in the same Tripwire Enterprise console which allows for the same evidence of the change to production to be collected. Date and timestamps are used to demonstrate that the change occurred in the test environment prior to production (CIP-010 R1.5).

After the baselines were well established within Tripwire Enterprise, we focused on expanding our use of Tripwire to include testing of CIP-005 and CIP-007 Security Controls (CIP-010 R1.4 and CIP-010 R1.5). Engineers worked to identify the security controls for given devices. Policy Testing was then configured in the Tripwire Enterprise application to test the identified security controls.

When changes occur to the devices in Tripwire, the results of the policy tests are updated automatically and evidence of the testing is collected as part of the change to the baseline. This allows the security controls testing to be automated and consistent across changes regardless of the device or the personnel performing the change.

Thanks to Tripwire and the processes developed around it, NIPSCO OT is able to comply with a number of requirements as efficiently and cost-effectively as possible.

Internal Controls - Part II

By: Denise Hunter, Senior Technical Auditor

What are Internal Controls and are they needed?

As you know from previous articles and our workshops, we've identified internal controls as any activity that you perform to ensure that what you want to happen, happens. By defining and designing strong, appropriate controls, both large and small entities can improve their compliance posture and should recognize benefits across their organization. A properly designed internal control will provide numerous benefits, a few of which are: identifying areas of risk prior to the risk escalating to an event; providing a paper trail (tangible or electronic) substantiating compliance for any compliance oversight engagement; identifying areas of interdependence that you may not be aware of; and providing organizational transparency to help reduce silos and increase cross functional awareness.

Types of Internal Controls and their benefits:

Preventive Controls. These are proactive controls. Preventive Controls are focused on quality and function to identify misinformation, irregularities, or errors. They are often considered extremely effective because they are based on company objectives, are usually inexpensive to implement, and assist in maintaining assets.

Examples of preventive controls include:

- Segregation of duties: more than one individual completing a task
- Approvals: confirmation of calculations, transactions, or activities by independent review
- Authorizations: delegation of duties
- Verifications: ensure the accuracy, correctness, or truth of the information
- Asset management: inventory of assets with defined attributes

Detective Controls. These are controls that are designed to identify errors and irregularities after they have occurred. They help identify issues when a preventive control has failed.

Examples of detective controls include:

- Peer reviews
- Data reconciliations
- Internal audits

Corrective Controls. These controls are triggered when a detective control has identified an issue. Corrective controls help to identify activities that should be implemented to rectify an issue and hopefully prevent it from happening again. Corrective controls often become the new preventive control.

Examples of corrective controls include:

- Implemented procedures
- Data backups used for recovery

A dynamic internal control program would consist of controls from all three types.

Components of an Internal Control and Internal Control Program

A properly designed internal control will:

1. Identify the line of demarcation; what event triggers the internal control activity to commence and when is the control completed
2. Sequence all activities that must occur to perform the internal control, focusing on only 'key' activities
3. Determine information or data needed to perform those activities and where to get that information
4. Determine internal control output
5. Identify all stakeholders (internal and external) the control outcome must be reported to
6. Assign ownership of each internal control to the appropriate position
7. Be documented, either as a procedure, checklist or flowchart

A strong internal control program possesses:

1. Competent, empowered personnel
2. Clear flow of communication, both vertically and horizontally
3. Segregation of Duties or appropriately implemented reviews, in order to reduce the likelihood of errors or irregularities
4. Appropriate documentation and record retention
5. Monitoring of the internal control program to ensure controls are appropriate and operating as designed.

Internal Control Limitations

No internal control or internal control program is ever perfect. The largest risk to any internal control program is human error. Humans are inherently fallible. For example, cognitive bias, or seeing what you expect to see while performing a mundane or frequent task, poses a large risk to the organization. However, this risk can be mitigated either by Segregation of Duties or inserting a performance review between key processes.

Balancing the cost of a specific control for the expected benefit of the control should be considered when designing an internal control program. Some controls cost next to nothing to implement (reviews, standardized documentation, reconciliation of supporting documentation to information captured within software programs). However, that is not true for all controls.

Finally, internal controls should be assigned to a position, not a person. This ensures a continuation of the control when a person is absent from their position, establishing a practice where specific tasks assigned to a position continue to be performed. By implementing this process, you shift the posture of the organization from being 'Person Dependent' to 'Process Dependent,' reducing some of the risk faced by the organization.

By: PJM Interconnection, LLC

PJM powers through hotter-than-usual summer, keeping the lights on for 65 million people

The summer months see the highest peak electricity usage of the year, and the 2018 season was forecast to be hotter than usual in the PJM footprint.

PJM was ready to meet demand and keep power flowing to the 65 million people it serves in 13 states and the District of Columbia.

Last summer, demand peaked at 145,331 MW on July 19. This year, PJM surpassed that on June 18 – a few days before summer officially began – with a peak usage of 149,170 MW.

PJM planners had forecast a peak demand of 150,000 MW for the season. To put that into context, the RTO's all-time highest power use was 165,492 in the summer of 2006.

PJM keeps the lights on through its competitive markets, planning and operations. It also relies on the preventative maintenance that more than 1,000 members perform on their equipment all year round so that it's up to the task of handling peak summer loads.

PJM meets electricity needs by procuring enough resources to satisfy peak demand plus required reserves at the lowest reasonable cost through its competitive markets.

"PJM continues to ensure that the power supply is secure and reliable while maintaining efficient and transparent markets that save billions of dollars for our customers," said Andy Ott, president and CEO. "We have planned and prepared for summer operations and we have plenty of reserves to meet the demand."

Throughout the summer, PJM also uses Hot Weather Alerts to coordinate the flow of energy with utility partners and avoid capacity problems on the grid.

Sometimes, these alerts are specific to zones; other times they are system-wide. Since June 18, four RTO-wide Hot Weather Alerts have been issued.

Such alerts prepare transmission or generation personnel and facilities for extreme hot and/or humid weather conditions that may cause capacity problems on the grid. Transmission and generation operators determine if any maintenance or testing on their facilities can be deferred to a later date or even canceled.

PJM also has resources on reserve to cover generation that is unexpectedly unavailable or demand that is higher than forecasted. PJM's required reserve is 16.1 percent of the forecasted demand level, and this summer PJM's expected reserve margin is more than 28 percent, or nearly 41,000 MW. PJM has 184,010 MW of installed generating capacity available. (One megawatt can power about 800 homes.)

At PJM control centers, experts monitor, control and direct the power grid 24/7 with sophisticated technology to balance supply and demand. They adjust the production of generating plants to changes in demand, and make sure that no transmission lines or facilities are overloaded. The system operators also watch for unusual conditions and react to them to protect the electricity supply.

Working together with its members, PJM ensures that the largest power grid in the U.S. has ample electricity to power through the summer – no sweat.

Small Entities and Compliance

By: Glenn Kaht, Principal Technical Auditor

RF works and interfaces with entities of all sizes, ranging from large utilities and RTOs to small entities (typically GOs and GOPs, DPs, and even some TOs). This article discusses some of the challenges that small entities face, and provides suggested solutions to those challenges. The topics covered are based on RF's experience working with many small entities, primarily through compliance audits.

There is no definition for a "small entity," but a small entity is generally recognized as an entity that has a limited amount of Bulk Electric System (BES) facilities and compliance obligations, and a lesser impact on the reliability of the BES. Even though a small entity has a lesser impact on the reliability of the BES, they do have an impact, and that impact increases when the small entities are aggregated. As a result, it is important that small entities maintain compliance with Reliability Standards (Standards), maintain, and operate their facilities in a manner that supports the reliability of the BES.

Small entities typically have limited resources available to dedicate to compliance. The individual responsible for ensuring compliance is frequently performing dual functions, such as a plant operator, plant manager, or plant engineer, in addition to their duties of ensuring compliance. The individuals responsible for compliance need to keep up with compliance obligations associated with current and new Standards. RF provides various resources to help small entities keep up with these obligations. These resources include the monthly compliance update letter, the RF newsletter (which you are reading now), our Reliability and Compliance Open Forum calls, and workshops/seminars. RF encourages all entities to use these resources. Finally, if an entity still has questions, they can request an assist visit with RF to help understand their compliance obligations.

When conducting audits, it is not uncommon for an audit team to find that a small entity is unaware of all of their relationships with other functional entities. As an example, if a Standard calls for an entity to submit data to their TP, the entity needs to know who their TP is in order to maintain compliance with the Standard. All registered entities need to be aware of all of their relationships with other applicable functional entities (such as the applicable TO, TOP, TP, PA, etc.). If an entity is not aware of all of their relationships with other functional entities, the entity should reach out to obtain this information. This information can usually be obtained from an entity that they know they have a functional relationship with. Typically a smaller entity knows who they are interconnected to, such as the TO. Starting with that entity and moving up through to BA and then RC seems to have helped other smaller entities. If the entity is unable to obtain the information this way, the entity should contact RF to obtain this information.

Small entities are audited less frequently than large entities. It is not uncommon that the individual responsible for compliance was not involved with the previous audit. When an individual assumes compliance responsibility for an entity, he/she should be aware of the results of past audits, including any findings identified in the audit. When compliance responsibility is transferred from one individual to another, there should be a complete transfer of prior audit results, and where all the compliance related materials are being retained. This should help with a smooth transition of duties.

It is common for a small entity to not have in house expertise to perform all required compliance activities per the Standards. Examples include performing maintenance activities on Protection Systems (PRC-005), coordinating generator voltage regulating system controls (PRC-019), or providing verified models for generators (MOD-026 and MOD-027). When a small entity does not have the in house expertise to perform the actions necessary to ensure compliance, a third party vendor is usually employed to perform activities to help ensure compliance of the small entity. The entity should ensure that the third party is going to perform the activities that are necessary to ensure compliance, and after the activities are performed, the entity should ensure (via a review) that the required activities were performed to expectations. The individual responsible for compliance should have a sufficient understanding of the work performed, and the documentation provided by the third party to be able to discuss and demonstrate compliance to an audit team.

While the focus of this article is not to discuss internal controls, it should be noted that internal controls could be designed and implemented for all of the issues discussed above. It is not necessary for a small entity to have an elaborate internal control program. However, the level of internal controls should be commensurate with the complexity of the compliance obligations of the entity. Small entities can design and implement relatively simple internal controls to achieve the desired compliance obligations and reliable operations of the entity.

Small Entities and Event Analysis

By: RF EASA Department

Less than four percent of the 390 events we reviewed across the RF Region over the last four and a half years affected small entities. The infrequency of these events makes sense, since:

1. it would be uncommon for a Generator Owner/Operator with a small fleet or a Distribution Provider to cause an event that results in significant load loss, cascading, instability, separation, or voltage reductions; and

2. smaller entities typically have limited monitoring of their own assets without widespread models or advanced functionality such as state estimation, real-time contingency analysis, or voltage stability analysis, which results in very few EMS-related outages.

However, events still occurred and RF wants to ensure all our entities understand what to look for and report when unplanned events take place. Therefore, below is some information based on the 15 events that did take place at smaller entities and some reminders for the process so you know how to respond should you encounter one.

Recent events impacting smaller entities are detailed below:

- Two events involving the ***unplanned loss of three or more generating units*** by a common disturbance (category 1a),

- Two ***unplanned control-center evacuation events*** (using the retired category 1f or currently category 0 for an uncategorized event),

- Eleven ***physical security events*** involving either suspicious activity or vandalism at the facility (reportable, but uncategorized in the Events Analysis program, category 0).

Category 1a events, including the loss of three or more units, but which can also include the loss of three or more transmission lines, are more common to larger utilities who own and operate more assets. In smaller entities, these types of events are typically due a protection system Misoperation.

When these happen, RF will ask you to submit a voluntary Brief Report to the Events Analysis & Situational Awareness Team (EASA). These types of events are then cause-coded in the Event Analysis Process where RF and NERC will work with you to analyze the event, determine the root and contributing causes, document mitigations, and discuss if there are any applicable Lessons Learned to share with industry.

EASA will help walk you through this process as these types of occurrences may be seldom for smaller entities.

Control-center evacuations (formerly category 1f events) are still reportable as per NERC standard EOP-004-3, however they are no longer categorized in the Events Analysis Process. While these are reported, tracked, and trended by ReliabilityFirst's EASA team, they are not often cause-coded and usually a Brief Report is not needed.

EASA may follow-up with you regarding the circumstances and any risks, but usually the necessary information is included with the written description in the EOP-004 Attachment 2 submitted here.

Physical Security Events are the most common 'small-entity' event. Usually these entail some type of suspicious behavior or vandalism at a substation. These may include someone taking pictures of your facilities, a break-in to steal copper, or even an unidentified drone hovering around a substation yard.

Continued on page 10

Small Entities and Event Analysis

Continued from page 9

While these are also not categorized in the Event Analysis Process (recorded as category 0 events), they are not to be taken lightly!

Recently, and very close to RF's headquarters, it was the detection of suspicious activity that led to the arrest of a man plotting a terror attack on the July 4th parade in Cleveland. While the EASA team typically does not ask for a Brief Report for these reportable incidents, there are certain things we are looking for on the EOP-004 Attachment 2 when a physical security event occurs:

- Was a police report filed?
  - Working with the authorities is an important internal control to help catch anyone who may be trying to harm the Bulk Power System.

- Did you investigate the station?
  - Sometimes it is assumed following a break-in that the perpetrator was only there to steal copper. It's important to perform a walk-through to see if any control handles, switches, devices, or any other important equipment was compromised.

- Is this a trend or emerging risk?
  - Because EASA receives multiple physical security reports, we can work with NERC (and E-ISAC) if we think there is a trend. Is this the first drone activity or the hundredth? Has this facility been targeted before? Was the facility housing a key generator, or part of a key interface that could cause harm to the BPS if compromised?

Hopefully this will provide an idea of the types of questions you can anticipate. If this information is documented in the written description of the EOP-004 Attachment 2, often these events can be closed out without any additional follow-up required or needed. Otherwise, RF's EASA team may collaboratively reach out to you with any questions.

For more information about the Event Analysis Process, please see the EASA section of our public website located here We draw your attention to two important links:

1. Event Reporting which has additional details about how/when a report needs to be submitted.
2. Guidance on Category 0 Events which provides some guidance on what to expect for events that do not fit into the NERC Event Analysis Process (such as the physical security events).

One of the main deliverables of the Events Analysis Program is the creation of Lessons Learned documents. NERC recently published a new Lessons Learned document that may help small entities regarding guidance for entities with low-impact cyber assets.

For any questions about how the Lessons Learned process or how these recommendations can improve your internal controls, please feel free to reach out to any member of the EASA staff.

Document Management Best Practices

By: Rhonda Bramer, Principal Technical Auditor

Documenting business processes is one of the most critical activities for compliance. The more information that you can collect and document in your process, the better chances you will have that it is accurate, understood, and followed. Producing quality/good documentation is a collaborative process that involves the input of more than one individual.

Creating and updating process and procedure documents is a critical business process that should include peer reviews before final publication and during annual reviews. Peer reviews foster collaboration and help maintain quality standards, improve performance and provide credibility. Engaging someone unfamiliar with the process to review and ask additional questions can help validate the content and confirm completeness.

Why is good documentation important? It reduces operational ambiguity. Good process documentation reduces confusion regarding who is supposed to do what or how it is supposed to be done. These documents serve as the collective organizational knowledge and are able to be accessed and followed as needed.

Good Documentation Practices

How do you know if your documentation is accurate and adding value to the process? Engage operational staff and utilize peer reviews to complete specific tasks by following the process you documented. Sometimes, it's easy to accidentally leave out important details because you're so accustomed to the process that you're doing it on autopilot. Stepping back and allowing someone else to work through the documentation will reveal whether you have missed any critical details.

Add Visuals

Visuals are key to creating good documentation. We've all heard that a picture is worth a thousand words, but in documentation, they just might go beyond that. Whether it's a screenshot or a flow chart, these will help guide any staff member through a variety of processes. Without visuals, your documentation can become subject to misinterpretations and delays in finding the correct next step.

Beyond the visuals, make sure that the language being used in your documentation is just as helpful. Writing processes clearly is imperative for your documentation success, and it doesn't have to be difficult. Simple steps like avoiding passive voice, being concise, and making sure to move from start to finish, go a long way towards creating good documentation.

Attributes to good documentation

- Information is organized logically
- Content is relevant and accurate
- Aligns with best practices
- Format and layout is easy to scan and read
- Uses appropriate graphics and tables to support the text

6 Criteria for Good Documentation

- Clear
- Concise
- Correct
- Accurate
- Accessible
- Complete

The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

Cybersecurity and CIP for Small Entities

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'm at a small company and I've been tasked with creating a cybersecurity and CIP compliance program. Where do I start?

A There are a number of resources available to help you on your way. Since you are a small entity, I will assume for this article that you are in the CIP program at the low impact level, although most of my suggestions will be applicable to the high and medium impact levels as well.

I suggest you begin with a basic Information Technology (IT) program and then adapt it to your Operational Technology (OT) environment. As you build your program keep the CIP Standards in mind. I feel it will work best if you build the CIP Standards into your security program, as opposed to building a security program around the CIP Standards. In other words, a good cybersecurity program should go far beyond the minimum requirements of the CIP Standards, while maintaining compliance with all aspects of those Standards.

If you're new to cybersecurity, a good way to start is with a class on the fundamentals. If you need advice on choosing a class, send me an email at the address below.

Books

If your budget or your schedule won't accommodate a class, start with a basic book on IT security. One example of an introductory book I've found useful is "Defensive Security Handbook" (2017, O'Reilly Media Inc., ISBN 978-1-491-96038-7). This walks you through building a cybersecurity program from the ground up, although it does not deal with Industrial Control Systems (ICS).

St. Joseph, MI – Photo: L Folkerth

To build ICS capability into your cybersecurity system, a book like "Hacking Exposed – Industrial Control Systems" (2017, McGraw Hill Education, ISBN 978-1-25-958971-3) is one possible choice. In particular, the first chapter provides an excellent introduction to ICS security. RF will post a list of books and resources you may find useful in the upcoming CIP Knowledge Center on our website.

CIS "Top 20" Controls

As you are working through understanding your environment, a key facet of your cybersecurity program will be a set of security controls. You can start with a set such as the "Basic CIS Controls," available for free at

	CIS Control	CIP Standard
1	Inventory and Control of Hardware Assets	CIP-002-5.1 R1, BES Cyber System Categorization
12	Boundary Defense	CIP-003-7 R2 Att 1 Section 3, Electronic Access Controls
17	Implement a Security Awareness and Training Program	CIP-003-7 R2 Att 1 Section 1, Cyber Security Awareness
19	Incident Response and Management	CIP-003-7 R2 Att 1 Section 4, Cyber Security Incident Response

Continued on page 13

Continued from page 12

These controls, also known as the "Top 20," may be adapted as needed to your OT environment or adopted as a whole for your entire organization. Because the "Top 20" deal with IT environments, you should also read "Implementation Guide for Industrial Control Systems," available at here in order to adapt the Basic CIS Controls to your control systems environment.

At the low impact level, the CIS controls in Table 1 (on the previous page) have applicability to the CIP Standards.

US-CERT/ICS-CERT

While not required by the CIP Standards at the low impact level, your security program should include vulnerability management. This will enable you to address weaknesses in your security posture before these weaknesses are exploited by malicious actors. The U.S. Cyber Emergency Response Team (US-CERT) tracks and alerts on vulnerabilities in the IT environment while ICS-CERT does the same for control systems.

You can sign up for alerts here and here. ICS-CERT also has a good overview of ICS vulnerabilities here.

ICS-CERT goes beyond vulnerability alerts in offering free training. The available training ranges from introductory videos to instructor-led classes (also free, except that you must pay your own travel expenses), culminating in an advanced five-day hands-on class. More information on ICS-CERT training is available here.

CSET

As you get deeper into your cybersecurity program, you will want to conduct evaluations of the program. A valuable tool for our industry is the ICS Cyber Security Evaluation Tool (CSET) provided for free by the National Cybersecurity and Communications Integration Center (NCCIC), an organization within DHS. This tool helps you to perform a self-assessment of your control system security posture, and goes into detail about your control system networks and how they are protected. CSET is a Windows application that you will download and install on a local PC.

It includes a network diagramming tool so that you can easily describe your control systems network to the tool. CSET will ask you a series of questions regarding your security practices. The final result is a set of reports that will provide details about the results of the assessment (see Figure 1 for a sample page).

CSET has the ability to take the CIP Standards into account in its assessment. This capability could be used to give you a more accurate picture of your security and compliance posture. CSET does not directly support low impact at this time, but you can select standards for high and medium impact that will address the low impact requirements.

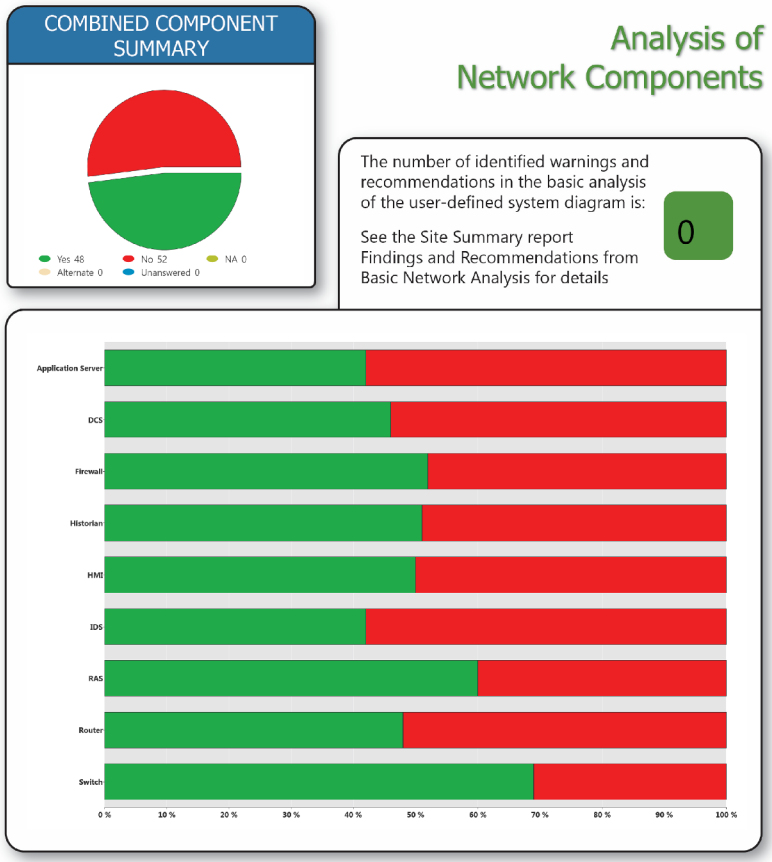


Figure 1

NIST CSRC

The National Institute of Standards and Technology (NIST) operates a Computer Security Resource Center (CSRC). The CSRC has many publications (read here) which are useful for our cybersecurity efforts. One of the most popular CSRC publications is Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*. This 462 page document contains an exhaustive set of controls for implementing IT

Continued on page 14

Continued from page 13

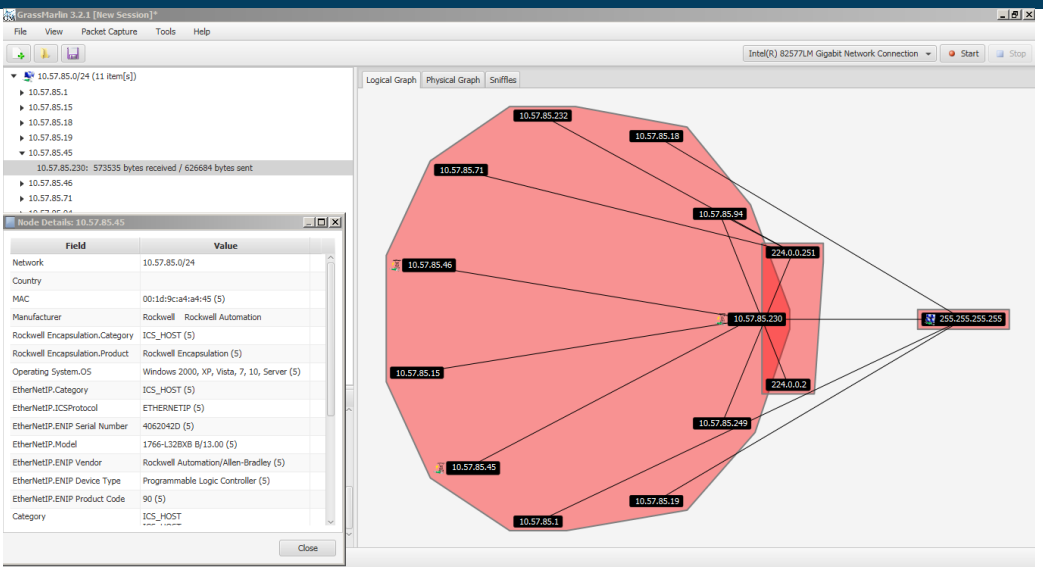


Figure 2 - Grassmarlin

security and is used, among other things, to implement security controls in the US Government.

I recommend that you download a copy of SP800-82, *Guide to Industrial Control Systems (ICS) Security*. SP800-82 contains an excellent comparison of IT and OT security in Section 2.4. Chapter 4 discusses development of an OT security program, and Chapter 5 provides an in-depth look at designing a security architecture for OT systems.

Security Onion

Security Onion is a special-purpose version of the Linux operating system that performs monitoring and recording of network traffic using standard PCs. CIS Control 12, Boundary Defense, contains sub-control 12.5 which calls for configuration of monitoring systems to record network packets. Monitoring and recording network traffic is also an element of incident response, required by CIP-008-5 for high and medium impact BES Cyber Systems and by CIP-003-7 R2 Attachment 1 Section 4 for low impact BES Cyber Systems.

There are some very good commercial products available to do this, but those products can also be expensive. Security Onion is available for free here.

GRASSMARLIN

GRASSMARLIN is another free tool used for network monitoring, but GRASSMARLIN differs from Security Onion in that it is designed to passively monitor ICS networks and identify ICS systems and traffic patterns on those networks. Passive monitoring is important in ICS environments due to the sensitivity of some ICS systems to any change in the network environment. GRASSMARLIN can be used to monitor for unexpected or unwanted patterns of traffic, and can also be used as a discovery tool for ICS devices.

This can be useful in CIP-002 to ensure you have inventoried all of the systems that can have a 15-minute impact on the BES. GRASSMARLIN can identify ICS devices by network traffic analysis.

Figure 2 shows the result of a GRASSMARLIN monitoring session on a small test network. Note the control system icon next to three of the devices on the network. This denotes a device that is communicating with one or more ICS protocols, making it a subject of interest in the identification and protection of control systems.

GRASSMARLIN was developed by the NSA and is available for free here. This web page also has links to the User Guide and to a brief slide deck on the capabilities of GRASSMARLIN.

Security Testing Environment

You should not implement any of these tools directly into your control system environment. First, you should first familiarize yourself with the operation of each tool. You should understand the possible impact of each tool on your production environment.

If you don't already have one, I strongly suggest that you set up a security testing environment to try out and evaluate any tool you plan to incorporate into your security program.

It is possible to set up your own security testing environment without expending a lot of resources. A couple of ICS devices and a small PC can provide a lot of benefit if your company can't afford a full test environment. Figure 3 (on the next page) shows my personal testing environment as it was used to test GRASSMARLIN. The used PLCs were obtained from eBay, the Ethernet hub from a garage sale, and other components from commercial sources. The wood backboard and legs (actually shelf brackets) were obtained

Continued on page 15

Continued from page 14

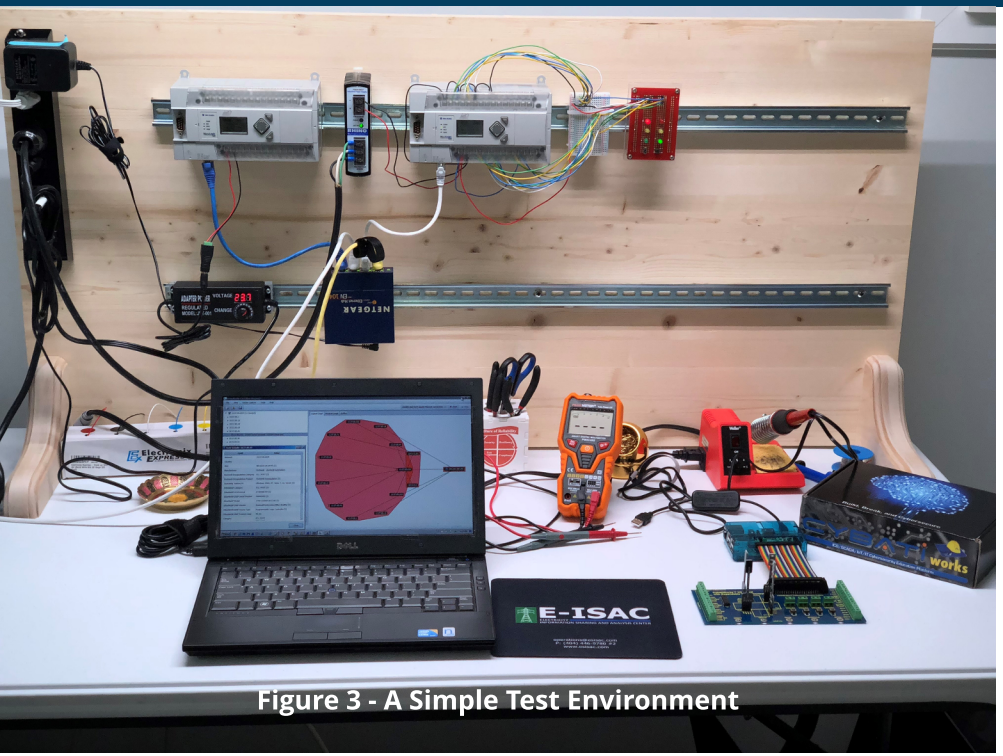


Figure 3 - A Simple Test Environment

from my local Lowe's. Except for the PC, which is an older repurposed laptop, the entire setup cost less than $500.

RF Knowledge Center – CIP

There are many resources available in addition to those I describe above. In recognition of this, RF is establishing a CIP area within the Knowledge Center on the RF website. We will update the CIP Knowledge Center with resources and links to resources for CIP compliance and ICS cybersecurity that we believe may help our entities. An expanded version of this article will be posted there as well.

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.

Newsletter Correction

In our previous issue, an error was discovered in the Lighthouse article regarding the initial implementation date for low impact Cyber Security Incident response plans.

We promptly identified and corrected the pdf, but if you downloaded the original version of the May/June newsletter, please be aware of the correction to avoid any confusion.

Feedback

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

I may be reached here.

In the Industry

NERC Publishes Updated User Guide on Self-Reports & Mitigation Plans

In June 2018, NERC, in coordination with the Regions, published an updated "Registered Entity Self-Report and Mitigation Plan User Guide" (User Guide), available here. This User Guide describes the type and quality of information that entities should include in their Self-Reports and Mitigation in order for the Regions to effectively evaluate the risk of the potential noncompliance and activities required to mitigate the risk and prevent recurrence.

Below is a non-exhaustive list, including information from the User Guide as well as RF's experience, of key information to include in Self-Reports and Mitigation Plans: *For more information on root cause analysis, *see* User Guide, Appendix D.

SELF-REPORTS

An adequate Self-Report includes at least the following information:

- How the noncompliance was discovered (e.g., detective control, internal review, audit preparation activities, or an event).
- If the noncompliance was *not* discovered through an internal control, whether or not there were controls in place that would have eventually detected the noncompliance.
- When the noncompliance was discovered (which is different than the date the entity determined the issue was a potential violation of a Reliability Standard).
- When the noncompliance began (which is not dictated by the discovery date) and ended, or will end.
- Comprehensive description of the issue (tell your story).
  - Series of events leading to noncompliance; scope of and facts and circumstances surrounding noncompliance (number of people, assets, or facilities impacted; function of assets; size of facilities and potential impact on grid; system condition at time of noncompliance; actual harm; and other protections in place to potentially mitigate risk).
- Preliminary root cause determination. (Note: human error is rarely the root cause.)*
- All relevant internal controls.
  - If the entity implemented internal controls, describe how effective the controls were at preventing, detecting, and correcting the noncompliance prior to the manifestation of harm. Remember, a control could be a process, procedure, system, or a tool and could be implemented in an automatic or manual manner.
- Steps taken to address immediate potential risk of noncompliance and other known completed or planned mitigating activities.

MITIGATION PLANS

Entities may submit Mitigation Plans or mitigating activities, but, regardless of which path an entity chooses, the entity must: (a) correct the noncompliance, (b) address the root cause, and (c) take steps to prevent recurrence.

The User Guide explains the circumstances under which a Mitigation Plan or mitigating activities should be used and their requirements. If an entity submits a Mitigation Plan, the Mitigation Plan should address the following:

- Scope and description of the noncompliance (even if already stated in the Self-Report or other initiating document).
- Detailed root cause analysis.
- Detective, preventative, and corrective actions.
- Descriptive milestones (if mitigation extends more than three months into the future).
- Expected completion date.
- Actions to address interim risk.

In addition to the User Guide, RF periodically provides additional outreach regarding effective Self-Reports and Mitigation Plans, such as webinars and targeted, one-on-one training with entities as needed or requested. Please contact RF's Enforcement Department with any questions.

Lean Operation Success Story

Scott Etnoyer's Team recently won the Talen Energy Spotlight Award for their work on improving the NERC Compliance program.

It recognized the high performing team for their performance that made exceptional contributions to the company's goals and had substantial cost savings for the company.

His team was able to do this by utilizing the RF assist visits and other regional programs that reduced legal and corporate reviews.

In addition, Talen's NERC team focused on ways to minimize review testing and verification work on the technical standards by standardizing testing and verification forms.

Regulatory Affairs

By: Larry Bugh, Director EASA & Chief Security Officer

Department of Homeland Security Reporting of Russian Hacking

Department of Homeland Security (DHS) officials in a July 24 webinar said that Russian-backed hackers infiltrated a power plant industrial control system (ICS) in an incident that could have caused a blackout last year.

As one might expect, this announcement prompted responses from Congress, the industry, and security researchers.

According to the report, Russian-backed hackers gained entry into control system environments in electric utilities as early as 2016 and then remained dormant in those systems in what is known as an Advanced Persistent Threat. They gained access using phishing campaigns against vendors used by the electric utilities. After capturing user credentials of the vendors, the attackers were then able to start traversing into the control system environment of the utilities, again using phishing campaigns to obtain valid user credentials inside the control environment.

According to the DHS briefing, the attackers successfully infiltrated a large number of electric utility control environments where the briefer stated they could have flipped switches and disrupted the grid. However, a follow-up statement by a DHS assistant secretary indicated, "To be clear, there was no threat for the electrical grid to go down. … While they were in a position to be able to manipulate some systems, there wasn't a broader threat to our entire electric grid." As more information has been released, in fact it appears that a wind power generator was the only entity that could have been controlled through the attack. Also Christopher Krebs, undersecretary for DHS's National Protection and Programs Directorate, stated, "That was a very targeted threat at the electricity subsector; for the most part, the defenses across the system worked."

What can we learn from this information? First, that the electric infrastructure is really a potential target of hackers, especially nation-state backed hackers. The Electricity Information Sharing and Analysis Center (E-ISAC) issued a non-public alert in June of 2017 concerning the activity, providing the industry with notification. However, the alert was provided to U.S. utilities 17 days after Canadian officials provided information to Canadian entities. This points to the need for continued improvement in information sharing between critical infrastructures and government organizations.

Second, as stated by Christopher Krebs, for the most part the defenses across the system worked. So, the work our utilities have performed to address the risk of cyber security has borne good fruits. However, on August 2, 2018, security firm Dragos reported on a new hacking effort targeting at least one U.S. utility and using methods that appear very similar to the methods reported by DHS in the 2017 campaign attributed to Russian-backed hackers. Bottom line, cyber security is not a destination, but a journey and we must continue to be vigilant and improve defenses as technology evolves.

From the DHS analysis of the 2017 campaign, one of the tactics the attackers used was simply visiting public web sites of target entities looking for photos on those web sites, But not just any photos. The focus was photos that were PR-type photos that may have included backgrounds such as control rooms or other backgrounds that might reveal more information about the control systems than any utility would have intended. With advancements in photo technology, a user can zoom in on high resolution photos and be able to clearly view information that may not have been the intent of the photo. In the case of the hacking campaign, the photos that were downloaded by the hackers contained information in the background of those photos that revealed data about the control systems in use. Entities should be cautious of information they publish for public consumption to ensure they do not reveal more information than intended.

FERC to Expand Cybersecurity Reporting Requirements

FERC issued a final rule directing NERC to develop and submit, within 6 months, modifications to the CIP Reliability Standards to augment mandatory reporting of Cyber Security Incidents, including incidents that might facilitate subsequent efforts to harm the reliable operation of the nation's BES. This broadens the scenarios for reporting from the current rules that require reporting if one or more reliability task is disrupted or compromised.

The Final Rule directs NERC to develop and submit modifications to the Reliability Standards to require reporting of Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's Electronic Security Perimeter or associated Electronic Access Control or Monitoring Systems that perform certain functions. FERC states that NERC should include minimum attributes in reports and develop reporting timelines for Cyber Security Incidents based upon the severity of the event and the risk to BES reliability.

FERC states that reports should also be sent to the Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team in addition to the E-ISAC. Finally, FERC directs NERC to file an annual, public, and anonymized summary of the reports with FERC. The Final Rule will take effect 60 days after publication in the Federal Register.

Standards Update

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

General NERC Standards News

Resources from Supply Chain Small Group Advisory Sessions Posted

NERC hosted small group advisory meetings with registered entities, Standards Developers, and Regional Entities to assess the implementation of the CIP Supply Chain Standards:

- CIP-013-1 (Cyber Security – Supply Chain Risk Management
- CIP-005-6 (Cyber Security – Electronic Security Perimeter(s))
- CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments)

The event consisted of two parts:

- General Sessions and Live Webinar: on March 14, 2018 from 1:00–3:00 p.m. a general interest session, including industry speakers and NERC staff was held to discuss supply chain issues and solutions.
- One-on-One Sessions: closed one-on-one discussions between a registered entity's supply chain security experts and Electric Reliability Organization (ERO) Enterprise staff about concerns pertinent to that entity's implementation of the Supply Chain Standards.

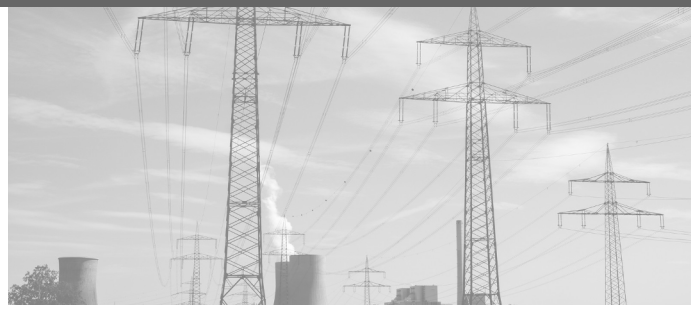
NERC has posted responses to frequently asked questions from registered entities as they prepare for implementation of the proposed CIP Supply Chain Standards.

Resources Posted

NERC has posted the slide presentation and streaming webinar for the June 29, 2018 Virtualization, Technology Innovation, and the NERC CIP Standards webinar.

NERC posted two new lessons learned addressing the following topics:

- Risk of Internet Accessible Cyber Assets
- Preparing Circuit Breakers for Operation in Cold Weather



Notable NERC Filings

In May, NERC filed the following:

- reply comments on the Federal Energy Regulatory Commission proceeding summarizing the manner in which resilience is a component of reliability, highlighting NERC Reliability Standards and other activities that support resilience, as well as emphasizing the importance of reexamining resilience in light of the changing generation resource mix and evolving cyber and security threats.

In June, NERC filed the following:

- an informational filing as directed in FERC Order No. 794, addressing: (1) an evaluation of the use of the linear regression methodology to calculate frequency response; and (2) the availability of resources for applicable entities to meet the Frequency Response Obligation.

In July, NERC filed the following:

- comments on the Notice of Proposed Rulemaking regarding proposed Reliability Standard TPL-007-2 (Transmission System Planned Performance for Geomagnetic Disturbance Events) issued by FERC on May 17, 2018; and,
- a petition for approval of proposed Reliability Standard PER-003-2 (Operating Personnel Credentials) and retirement of currently-effective Reliability Standards PER-003-1 and PER-004-2.

NERC's filings can be found here.

Standards Update

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

Notable FERC Issuances

In May, FERC issued the following:

- a notice of proposed rulemaking (NOPR) proposing to approve Reliability Standard TPL-007-2 (Transmission System Planned Performance for Geomagnetic Disturbance Events).

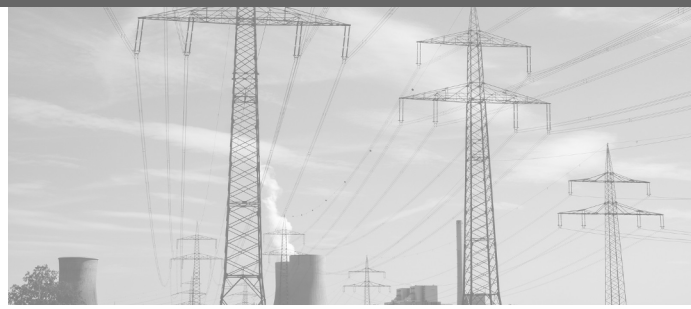
In June, FERC issued the following:

- a final rule approving Reliability Standards PRC-027-1 (Coordination of Protection Systems for Performance During Faults), PER-006-1 (Specific Training for Personnel), and the retirement of currently-effective Reliability Standard PRC-001-1.1, the associated Violation Risk Factors and Violation Severity Levels, and the associated implementation plans;
- a final rule approving revisions to section 400 (Compliance Enforcement), Appendix 2 (Definitions Used in the Rules of Procedure), and Appendix 4C (Compliance Monitoring and Enforcement Program) of its Rules of Procedure to incorporate the Consolidated Hearing Process, which provides a uniform and more streamlined approach to hearings for Regional Entities by giving Regional Entities an option to select NERC to manage the hearing process; and,
- a delegated letter order accepting NERC's filing of the Amended Compliance and Certification Committee Charter to reflect the participation of CCC observers in NERC audits of Regional Entities in accordance with Appendix 4 of the NERC Rules of Procedure.

In July, FERC issued the following:

- a final rule requiring expanded cyber security incident reporting. The Commission directed NERC to develop, within six months of the effective date of the final rule, modification to the Critical Infrastructure Protection Reliability Standards to improve mandatory reporting of cyber security incidents, including attempts that might facilitate subsequent efforts to harm reliable operation of the nation's bulk electric system; and,
- an order approving, in part, and denying, in part, proposed revisions to NERC's Rules of Procedure (ROP) sections 600 (Personnel Certification) and 900 (Training and Education).

FERC's issuances can be found here.



General FERC Standards News

FERC Open Meeting Action

FERC took action on several key reliability items at its July open meeting, including issuing a final rule on Critical Infrastructure Protection (CIP) Reliability Standards and an order on Rules of Procedure revisions.

FERC issued Order No. 848 directing modifications to the CIP Reliability Standards to improve mandatory reporting of cyber security incidents, including attempts that might facilitate subsequent efforts to harm reliable operation of the nation's bulk power system. FERC directed NERC to submit the modifications within six months of the effective date of the final rule.

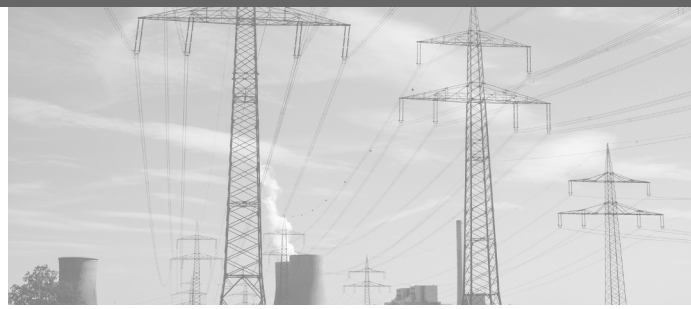
FERC also issued an order approving, in part, and denying, in part, proposed revisions to NERC's Rules of Procedure Sections 600 (Personnel Certification) and 900 (Training and Education). Specifically, the order directs NERC to restore sections 603, 604, and 605 that NERC proposed for deletion. These provisions pertain to:

1. procedures for suspension of an operator's certification (section 603);
2. dispute resolution process (section 604); and
3. disciplinary action (section 605).

The order determines that these provisions are not "programmatic detail" that can be transferred to NERC manuals but, rather, are substantive provisions that should remain in the NERC Rules of Procedure.

Standards Update

New Standards Projects



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

Project	Action	Start/End Date
Revisions to the NERC Standard Processes Manual	Additional Ballot Comment Period	7/31/18 – 8/9/18 6/25/18 – 8/9/18
Other Active Comment Periods		
Project	**Action**	**Start/End Date**
Comment Period Open for Version 3.0 of the Generating Unit Operations during Complete Loss of Communications Draft Reliability Guideline	Submit comments via email using the comment form	7/13/18 – 8/27/18
Recent and Upcoming Standards Enforcement Dates		
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 (Requirements 5, 5.1-5.2)	
April 1, 2019	EOP-004-4 – Event Reporting EOP-005-3 – System Restoration from Blackstart Resources EOP-006-3 – System Restoration Coordination EOP-008-2 – Loss of Control Center Functionality	
January 1, 2020	CIP-003-7 – Cyber Security – Security Management Controls 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)	
October 1, 2020	PER-006-1 – Specific Training for Personnel PRC-027-1 – Coordination of Protection Systems for Performance during Faults	

FERC Technical Conference

FERC held its annual technical conference on policy issues related to the reliability of the bulk power system on July 31, 2018.

The conference was comprised of four different panel discussions:

1. The Changing ERO Enterprise, Standards, and Reliability;
2. Advancing Reliability and Resilience of the Grid;
3. Managing the New Grid; and
4. Addressing the Evolving Cybersecurity Threat.

RF's President & CEO Tim Gallagher was a panelist on the "Changing ERO Enterprise, Standards, and Reliability" panel. Topics of discussion on this panel included:

- NERC's priorities for the next one to three years.
- The trends and risks identified in the 2018 State of Reliability Report and how to prioritize them.
- The status of NERC's effort to evaluate current Reliability Standards using a risk based approach to identify potential efficiencies through retirement or modifications of Standards.
- How the ERO has evolved and how it can be further improved including lessons from the experiences of the Regional Entities and NERC's benchmarking.
- The Western Interconnection's significant shift, with new Reliability Coordinations and the expansion of organized electricity markets.

- The status and efforts from the memorandum of understanding (MOU) with the Comisión Reguladora de Energía and the Centro Nacional de Control de Energía to establish a framework for a cooperative relationship between Mexico and NERC .

During the panel discussion, Tim Gallagher discussed RF's proactive efforts to improve reliability, including assist visits, maturity model evaluations, data analytics, and cold weather preparedness teams. He also discussed the recently issued 2018 CIP Themes Report, which identifies programmatic trends that create barriers to the CIP programs, and mitigation strategies for these issues.

What's Trending in Enforcement: Logging Tool Thresholds

In an effort to keep entities informed and help them proactively identify potential security and compliance issues, RF will periodically share potential trends it identifies through its compliance monitoring and enforcement work.

One issue that a few entities have recently experienced relates to logging tools. Logging is critical because it allows entities to not only investigate past physical and logical security incidents but also identify potential threats in real time.

An issue that some entities have recently experienced is their logging tools reaching the threshold for the number of logs they can retain, which results in the tools no longer accepting logs, or not being able to process the logs.

This can result from entities not verifying that tools have enough storage to meet the entities' needs, especially when the amount of storage needed may change over time. This issue can also result from improper configuration of the logging tools.

Thus, to prevent or reduce the risk of this issue, entities should periodically analyze the amount of storage required and then ensure that their tools have enough storage space and are properly configured to meet their needs. If you have any questions, please feel free to reach out to RF.

RF Board of Directors and Committee Meetings will be held at the RF offices in Cleveland, OH August 29-30, 2018.

Day One

The 2018 Reliability Fall Workshop will provide you with the opportunity to hear from two key ERO leaders. Jim Robb, who was recently appointed as NERC's President and Chief Executive Officer (CEO), will deliver the opening keynote speech and Tim Gallagher, President and CEO of RF, will close out the day. The workshop will also include NERC and RF subject matter experts presenting on a range of compliance and reliability topics such as; internal controls, misoperation trends, certification, and other related subjects. RF representatives will be available during breaks to offer one-on-one guidance and advice regarding your specific questions and issues.

Day Two

Compliance User Group (CUG) and Critical Infrastructure Protection Committee (CIPC) meetings will occur on day two.

Day Three

The 2018 CIP Workshop will cover a wide variety of topics with a focus on current threats and lessons learned from past events. A highlight of the workshop will be Chris Nissen, Director of Asymmetric Threat Response for the MITRE Corporation, who will be presenting on Supply Chain Attacks and Resiliency Mitigations. The workshop will also examine CERT Alert TA18-106A, regarding Russian State-Sponsored Cyber Targeting. Additionally, RF staff will present on regional Lessons Learned and provide an update on the Evidence Request Tool. To close out the day, two entities will share their recent experiences and best practices. RF representatives will be available during breaks to offer one-on-one guidance and advice regarding your specific questions and issues.

Calendar of Events

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

Date	RF Coming Events	Location
August 14-15	Protection System Workshop	Cleveland, OH
August 15-16	Human Performance Workshop	Cleveland, OH
August 20	Reliability and Compliance Open Forum Call	Conference Call
August 30	EMS Working Group	WebEx
September 17	Reliability and Compliance Open Forum Call	Conference Call
September 25-27	RF Fall Workshop	Cleveland, OH
September 26	RF CIPC Meeting	Cleveland, OH
September 27	EMS Work Group	WebEx
October 15	Reliability and Compliance Open Forum Call	Conference Call

Industry Events:

Date	RF Coming Events
August 14	BOTCC Executive Session
August 15	BOTCC Open Meeting
September 6	2018 Winter Weather Preparation Webinar
September 13	BOTCC Executive Session
September 20	FERC Open Meeting
October 2-3	NERC Monitoring and Situational Awareness Conference (at MISO)
October 15-19	GADS Conventional and Wind Training
October 18	FERC Open Meeting

New Jersey to Serve as a Public Sponsor and Board Member of National Offshore Wind Research Consortium

New Jersey will be a public sponsor and Board member of the National Offshore Wind Research and Development Consortium. The DOE selected New York State Energy Research and Development Authority (NYSERDA) to manage the $18.5 million Consortium. New Jersey, in conjunction with Rutgers University and the Center of Ocean Observing Leadership, has invested two million dollars in an Offshore Wind Modeling Initiative.

The Consortium's focus is to join industry, academia, government, and other stakeholders to advance offshore wind plant technologies, to create innovative methods for wind resource and site characterization, and to develop advanced technology solutions for installation, operation, maintenance, and supply chain.

The overall goal is to reduce the cost of offshore wind in the United States.

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