RELIABILITY FIRST

Themes and Lessons Learned

Compliance with the Critical Infrastructure Protection Reliability Standards

January 22, 2015

Table of Contents

PREAMBLE AND LIMITATION OF PURPOSE

Through its compliance monitoring and enforcement activities, and in coordination with North American Electric Reliability Corporation ("NERC"), ReliabilityFirst Corporation ("RF") has identified themes that have made it difficult for some entities to comply with Critical Infrastructure Protection ("CIP") Reliability Standards.[1] The purpose of this report is to communicate these themes, and possible resolutions to them, so that we can work together to continuously assure the reliability of the Bulk Electric System ("BES"). While there are many discrete valuable lessons learned published on NERC and Regional Entity websites to promote strong CIP performance, this report is intended to identify and share broader themes.

The suggestions for possible resolutions in this report are not, and should in no way be construed as, directives to industry to undertake any actions. Rather, most of these possible resolutions are merely approaches that have been successful for those certain entities. However, these possible resolutions may not be the best approach for every entity because the impact of the resolutions are largely driven by variables such as an entity's size, corporate structure, workforce, technology, culture, and other factors. Thus, before expending any resources to implement any of these possible resolutions, RF suggests that the entity perform a cost/benefit analysis that considers both the practical realities of their operations and themes identified in this report.

[1] The power industry is subject to mandatory Reliability Standards for Critical Infrastructure Protection. The entities discussed in this Report have worked with RF to resolve and mitigate any noncompliance with the CIP Reliability Standards. More importantly, all of these entities have voluntarily agreed to take actions that go above and beyond what is required to be compliant with the CIP Reliability Standards to further enhance the security of their operations.

I. EXECUTIVE SUMMARY

While entities seem to have been generally successful in developing and implementing compliance programs for the Operations and Planning Reliability Standards, some entities, large and small, seem to have initially struggled with developing and implementing compliance programs for the CIP Reliability Standards. During 2014 alone, RF received (through self-reports or self-certifications) or discovered almost 300 CIP Possible Violations. The ultimate goal behind the CIP Reliability Standards is to safeguard BES reliability by ensuring that cyber systems are operated and maintained securely. Although compliance alone does not guarantee secure operations, an entity's failure to maintain baseline CIP compliance may be indicative of an entity struggling to ensure the security of its system.

Through its compliance monitoring and enforcement activities, and in coordination with NERC, RF has identified themes that are consistently present with the more significant CIP compliance deficiencies. Generally, significant CIP compliance deficiencies are the result of multiple causes that overlap and are interrelated. So, while the themes discussed in this report are separated for clarity and ease of explanation, they are often comingled when analyzing an individual entity's CIP compliance deficiencies. The main themes RF has identified are:

a) the development of business unit compliance silos;

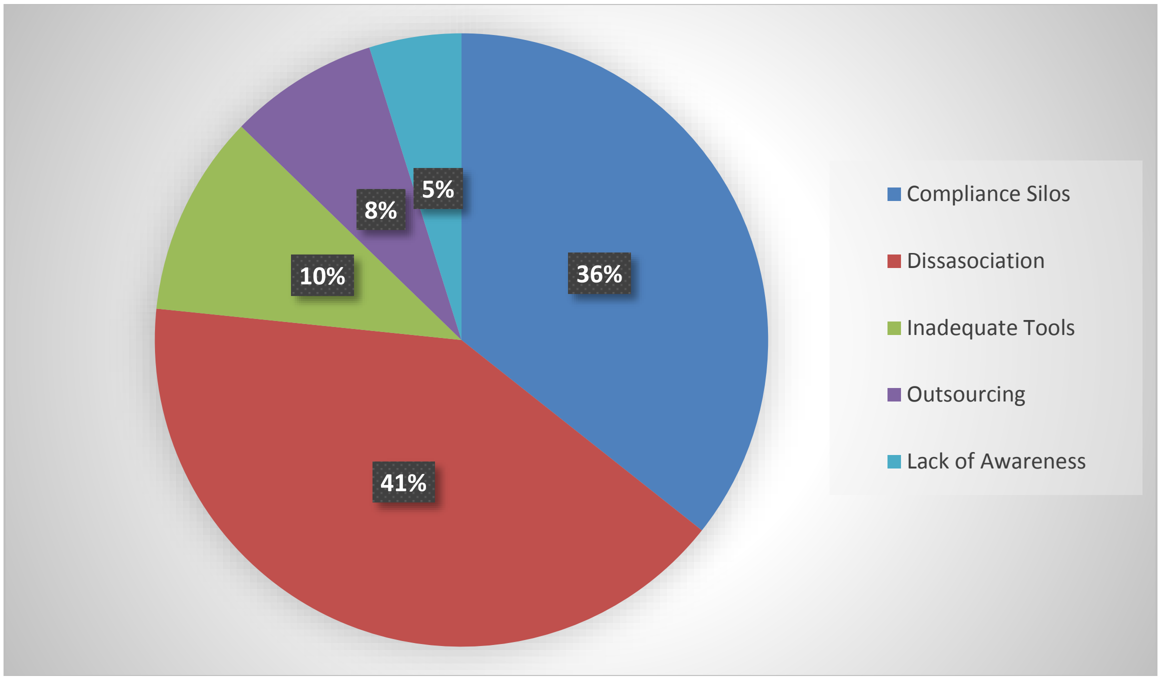
b) the disassociation between compliance and security;

c) inadequate tools or ineffective use of tools;

d) outsourcing core functions and compliance efforts; and

e) lack of awareness of an entity's systems or needs.

The following chart represents approximately 400 violations that comprise what RF considers to constitute the more significant CIP compliance deficiencies reported or identified in the RF region from 2010 through 2014 and indicates the number of violations caused, at least in part, by each of the identified themes. RF determined the significant CIP compliance deficiencies through consideration of the number of violations per entity combined with the severity of the risks posed by the violations individually or in the aggregate. As noted in the previous paragraph, some of the violations resulted from multiple causes and are thus included in the calculations for each contributing cause.



As the chart indicates, all of the approximately 400 violations that concern the more significant CIP compliance deficiencies are rooted in at least one of the five identified themes, with most of the violations rooted in entities developing business unit compliance silos and/or disassociating compliance from security. Below is an explanation of each of the five themes and suggestions on how to prevent their occurrence.

II. IDENTIFIED THEMES

A. Entities Develop Business Unit Compliance Silos

1. *Observations*

Several entities have experienced significant CIP compliance deficiencies as a result of a lack of internal coordination and uniformity that can be characterized as business unit compliance silos. These silos occur where entities fail to coordinate and/or consolidate compliance efforts across all business units and/or between departments. In one case, an entity had at least five different CIP compliance programs, including separate programs for its Energy Management System operations, Substations, Generation units, Human Resources department ("HR"), and Information Technology department ("IT"). Differing compliance programs within a single entity can lead to internal confusion, contradictions between processes, lack of ownership of projects or tasks, and other issues. Importantly, from a cyber security standpoint, silos may reduce security if the business units are not communicating with each other on such things as incident response, or there may be gaps in separate groups' incident response plans.

An entity's lack of departmental coordination can result in the entity's inability to successfully implement CIP-007-3a R3. This can occur where one department charged with patching the software does not coordinate with the department charged with configuring the software. Without this coordination, the tool used to identify whether the entity has the software for which the patch was released is compromised because firewalls may preclude its access to software behind those firewalls. RF has observed situations where entities failed to perform requisite software patching due to this lack of coordination.

This lack of uniformity and coordination can be especially problematic because many of the CIP Reliability Standards cross multiple business units or departments. For example, HR is usually one of the first departments, or the only department, to know when an individual's employment commences or terminates. The combination of this fact with inconsistent processes (or lack of processes) across HR and other business units routinely leads to an inability to successfully implement CIP-004 because the lack of coordination often results in unintentionally and improperly authorizing, or failing to revoke the authorization of, an individual's access to critical cyber assets.

The silo issue has also occurred at some larger Registered Entities where they implement both an overarching compliance program and individual compliance programs for each business unit. The issue arises where these individual programs are not coordinated with, and sometimes contradict, the overarching compliance program. As a result, the subject matter experts within individual business units had difficulty trying to reconcile which process to follow during implementation. This compliance program splintering tends to occur where upper management institutes processes in the overarching program that are not practical when applied to the operational needs of the individual business units.

2. *Suggestions to Address Compliance Silos*

To avoid inconsistencies, entities should consider coordinating compliance programs throughout the entity, including between departments, business units, and different levels of management. One way to coordinate compliance programs is to identify process owners that have the authority, ability, and responsibility to reach across business units to coordinate with other business units. Also, importantly, when developing procedures, management should work with those who implement the procedures to ensure that the procedures are practical. Demonstrating compliance should be a natural byproduct of an entity establishing procedures to ensure the secure operation of its system. If a compliance program is creating hurdles and is disconnected from practical reality (as opposed to being efficient and considerate of the obligations of the stakeholders), it is likely that compliance program splintering may occur, which leads to compliance inconsistencies and, ultimately, jeopardizes the secure operation of the system.

To assist in ensuring consistency across the entity, an entity's CIP Senior Manager should have a deep understanding of the entire CIP compliance program and the organization of the Business and should be able to identify any compliance silos that exist. The CIP Senior Manager should then assess the silos to ensure that they are appropriate for the entity's situation. For example, the Energy Management System department, IT, and the physical security group might have separate compliance programs due to being three different business units within the entity. Having three separate programs for these areas may or may not be appropriate, but if they are appropriate, the entity must ensure that the compliance processes and procedures are coordinated and well documented. Entities need to avoid situations where individuals or individual business units only consider their own responsibilities rather than the larger picture and how the business units must work together towards security and compliance.

Additionally, developing strong capabilities and performance in work management practices could assist the entity in coordinating multiple business units' compliance programs. Work management includes managing and integrating projects and operations in accordance with defined processes, collecting necessary information to monitor the projects and operations, and ensuring that all necessary people are available to support the projects and operations. An entity that has several compliance programs across multiple business units needs to manage and integrate those programs into the entity's overarching compliance effort to ensure that there are no gaps. Strong capabilities and performance in work management practices encourages the coordination necessary to manage multiple compliance programs across a single entity. RF is available to work with any of our entities to assess their work management practices on a voluntary basis, separate and apart from any compliance monitoring or enforcement activity.

B. Disassociation Between Compliance and Security

1. *Observations*

Issues often result from an entity disassociating compliance from security (and by extension reliability), which results in diminished value or emphasis on compliance. Some entities may at times view CIP compliance as merely a "paper compliance" exercise rather than viewing it as a baseline level of what an entity needs to do to maintain security, or, even better, as a natural byproduct of implementing an entity's procedures to ensure the secure operation of its system.

RF has identified problems where compliance and operations are concentrated in the same management or within one department, which becomes an issue if the manager has competing concerns (day-to-day operations versus compliance). For example, some entities charge IT with CIP compliance, but IT's primary responsibility is managing the entity's information systems, and thus compliance will likely take a back seat to IT's operational duties. The other issue with tasking IT to do CIP compliance is that while many of the CIP Reliability Standards relate to systems for which IT is responsible, compliance requires more than the ability to manage an entity's information systems. For example, CIP compliance requires knowledge relating to physical security and personnel and training.

As another example of an entity disassociating compliance from security, RF has observed a situation where an entity's NERC Compliance department, which was responsible for compliance for the entire enterprise, was tucked away in a single business unit within the enterprise. Management did not empower or provide the authority for that business unit to drive a consistent compliance program throughout the enterprise or across other business units. As a result, NERC compliance was not a priority among other business units, but rather, each business unit made its own operations a priority. Consequently, certain aspects of compliance went unaddressed due to gaps in processes, especially where, as stated above, the Reliability Standards apply across multiple business units or departments.

2. *Suggestions to Address Disassociation Between Compliance and Security*

Compliance efforts should be driven from the top down. To that end, if an entity's NERC compliance department is separate from other business units, it should either be located at the enterprise level or should have the authority to implement practices and procedures to ensure a consistent compliance program throughout the company. Alternatively, if an entity's corporate culture is such that compliance is made a priority, it may not matter where the compliance department is located within the corporate structure or how much actual authority the compliance department has over other business units. For example, RF has observed an extremely successful compliance program despite housing the compliance department in a separate business unit without much, or any, actual authority over other business units. The program works well because senior management has conveyed the message throughout the entity that compliance with the Reliability Standards is valued and necessary to ensure secure operations, thus enabling the compliance department to coordinate compliance efforts among business units and ensure all business units make compliance a priority.

Additionally, senior management should not only emphasize the value they place on compliance, but should be involved in compliance, even if at a high level. To get involved in compliance matters, management can: (a) hold periodic meetings with the individuals responsible for executing the compliance programs to stay apprised on current issues and monitor general compliance activities; (b) approve the compliance program and significant changes to procedures; (c) review and approve all self-reports, mitigation plans, self-certifications, and other compliance documentation; and (d) participate in or review internal assessment or audit reports. However, even if upper management is not directly involved in compliance matters, the CIP Senior Manager can be the link between the executive suite and the CIP compliance program and should have appropriate access to the executive suite and the board in order to keep these key positions informed regarding the status of the compliance program. In the event that the CIP Senior Manager uncovers compliance issues that need to be corrected, the CIP Senior Manager must receive appropriate executive support.

Another strategy to ensure the entity strives to achieve reliable operations, which are also compliant, is to write procedures and processes that go above and beyond what is required for CIP compliance. These processes and procedures allow and encourage the entity and its employees to focus on reliable operations rather than focusing merely on what is necessary to meet the CIP Reliability Standards.

Moreover, strong capabilities and performance in reliability quality management practices could assist in addressing an entity's disassociation between compliance and security. The purpose of reliability quality management is to provide objective insight into processes and associated work product related to BES reliability and security through objective evaluations of the quality of an organization's BES reliability and resilience activities. When an organization does not focus on reliability quality management, BES reliability and security may become secondary considerations. To maintain objectiveness and remove bias, individuals responsible for reliability quality management should be independent from individuals directly involved in operations. Also, effective reliability quality management practices include a mechanism for raising quality issues with senior management. Accordingly, an entity should designate an independent person or group to review an entity's work related to BES reliability and security so that the entity can ensure it is effectively implementing processes related to BES reliability and security.

C. Inadequate Tools or Ineffective Use of Tools

1. *Observations*

Another theme that RF has identified when entities experience significant CIP compliance deficiencies is an entity's inadequate tools or ineffective use of tools.

RF has observed entities purchase sophisticated tools, but fail to fully implement or properly configure those tools into their unique systems. For example, many entities have implemented tools to monitor account use under CIP-007 R5.1.2. However, entities sometimes fail to configure these tools in a way to aid the entity in detecting unauthorized access into their systems. To review individual account access, if the tool is not configured properly, the tool will produce voluminous logs that are impossible to digest in a meaningful way. Entities need to configure or "tune" these tools so that they can filter their log information to a useful summary as opposed to reporting large amounts of data. The purpose of the logs is to spot potential issues, but if the logs are too lengthy and include too much detail, the entity will almost certainly miss potential security issues within the logs.

2. *Suggestions to Address Inadequate Tools or Ineffective Use of Tools*

Automated tools can be extremely valuable in compliance and security efforts. In the CIP world, such tools as log management, intrusion detection, and configuration management, although initially expensive, can save thousands of hours of manual effort and can help detect deficiencies or security breaches that manual processes cannot detect. However, it is a mistake to think that it is possible to purchase a tool and install it with no additional work. Such tools must be configured for the intended job, with input from end users, and this configuration is almost never simple. Each automated tool will require an adequately trained staff, and management must allocate sufficient time for staff to analyze and configure the tool for best results. Consider the following illustration: you would not buy a new corporate aircraft and place an untrained person in the pilot's seat. An aircraft requires a skilled and trained staff to operate it effectively and safely.

To assist in ensuring that tools work as intended, entities should develop strong capabilities and performance in validation and verification management practices. Effective verification confirms that changes to the systems impacting grid reliability and resilience are conducted according to requirements, plans, or specifications, while effective validation confirms that changes to systems function as intended. Stated another way, verification addresses confirming changes to the system before they are implemented, and the validation process area addresses confirming changes after they are implemented but before becoming operational in the system. Thus, when an entity purchases a new tool, the entity's processes should require the entity to assess if and how it needs to configure the tool to work in its system as intended. Then, after the tool is implemented into the entity's system, the entity must confirm that it works as intended.

D. Outsourcing Core Functions and Compliance Efforts

1. *Observations*

Entities can experience issues with CIP compliance as a result of outsourcing core functions, such as IT, or compliance obligations generally.

Corporate IT departments typically support network infrastructure for departments within an entity and thus are often charged with executing certain CIP compliance efforts. By outsourcing core IT functions, an entity is relying on a third party not only to support network infrastructure from an operational standpoint, but in some cases also to ensure that the systems meet compliance obligations. An outside IT department generally cannot fully understand the needs, capabilities, and systems within an entity both from a personnel and technical level. Thus, there may be a disconnect between the outsourced IT services and the needs of the entity in terms of reliability activities (and by extension compliance obligations). Another issue with outsourcing is compliance sustainability and stability. As third-party engagements end, the knowledge surrounding the outsourced functions leave with that third party as opposed to keeping that knowledge with the entity.

Similarly, several entities have used third parties to draft mitigation plans. However, these third parties do not always fully understand the entity's limitations or internal system configurations. If the entity does not work closely with the third party to draft the mitigation plans, the mitigation plans cannot be tailored to fit the unique needs and systems within the entity.

Another problem that can arise from third parties drafting mitigation plans (or other compliance related documents, such as procedures) is a lack of ownership on the part of the personnel responsible for implementing the mitigation plans. A lack of ownership may be because the responsible personnel are not sufficiently familiar with the plans or may not understand the plans well enough to fully implement them as intended.

2. *Suggestions to Address Outsourcing*

Hiring third parties to assist in compliance and mitigation efforts can sometimes be useful and necessary, but entities must ensure that they work closely with the third party so that the compliance and mitigation plans are tailored to the entity's needs, capabilities, and systems.

RF recently observed an entity successfully use third parties to assist in mitigation plan development. This entity used a third party to assist in conducting root cause analyses and another third party to assist in developing the mitigation plans to cover those root causes. The entity worked very closely with both third parties throughout the entire process, so the mitigation plans were ultimately tailored to the entity's unique needs and systems. Additionally, despite using the assistance of a third party to develop the mitigation plans, the entity is intimately familiar with the mitigation plans and is taking ownership of the mitigation plans. In addition to helping to create the mitigation plans, the entity went through an exercise where its subject matter experts in charge of implementing the mitigation plans had to defend the mitigation plans to a panel of the entity's senior management and members of its compliance department. The entity then altered the mitigation plans as necessary and finalized the mitigation plans. This exercise helped ensure that the mitigation plans were tailored to the entity and that senior management and the individuals implementing the mitigation plans were familiar with and took ownership of the mitigation plans.

Likewise, developing strong capabilities and performance in managing external interdependencies can assist an entity in ensuring that the functions it outsources are tailored to its unique needs and capabilities. The purpose of external interdependencies is to implement organizational processes that manage external stakeholders that may impact BES reliability and resilience. When depending upon others to accomplish business objectives in the power industry, it is important to carefully consider all the dependencies that exist and manage the risks associated with outsourcing certain functions. For example, when outsourcing mitigation plan development, an entity has to manage the possible risks with that outsourcing, such as the third party's lack of understanding of the entity's technological capabilities. The entity needs to work closely with the third party to manage that risk. Similarly, if an entity chooses to outsource IT functions, the third party should first spend the necessary time to understand the entity's systems. However, it is also imperative that the entity manage ongoing risks of outsourcing IT functions, such as the third party not being aware of changes to the entity's systems. Thus, the entity should have a mechanism in place for notifying the third party of any changes to its systems. Further, the entity must understand and constantly monitor how the third party performs its contractual duties. Ultimately, the entity, not the third party, is responsible for reliable operations and compliance obligations.

E. Lack of Awareness

1. *Observations*

An entity's lack of awareness of how its systems work can result in significant CIP compliance deficiencies. The reasons for the lack of awareness can vary and might be the byproduct of one of the themes mentioned above, such as inadequate tools or outsourcing, or it could be that the entity does not have the experts it needs to fully understand its systems. This lack of understanding might be a result of inadequate funds to hire the right people or the entity not realizing it has a need.

For example, one entity thought it had adequate disaster recovery configurations because it had a mirrored back-up data center. However, because of the configuration, if the main data center was corrupted, the back-up data center would have also been corrupted within minutes. The subject matter experts did not understand their systems enough to know they had a significant CIP compliance issue. While the root cause of the entity's lack of awareness may vary, the lesson for entities is that they need to invest the time or financial resources necessary to fully understand their systems and where their systems may be weak. If entities do not have adequate resources, then they can seek guidance from others, such as RF.

2. *Suggestions to Address Lack of Awareness*

An entity has to understand why it has a lack of awareness *(e.g.* inadequate tools, inadequate personnel) before it can fix the problem. As Donald Rumsfeld explained:

> [T]here are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns -- the ones we don't know we don't know. And if one looks throughout the history of our country and other free countries, it is the latter category that tend to be the difficult ones.

Entities need to focus on the “known unknowns” and the “unknown unknowns” in order to understand where it is weak in its security posture. Designating a Senior CIP Manager who has sufficient understanding of the entity’s overall compliance and security posture could help better identify these “unknowns” by identifying areas of weakness.

If the problem relates to lack of appropriate personnel, strong capabilities and performance in workforce management practices can assist the entity in ensuring it hires the appropriate personnel to fit its needs and trains those personnel as appropriate. The purpose of workforce management is to ensure the ongoing suitability and competence of personnel to minimize the frequency and consequences of reliability and security events related to the BES. Workforce management includes establishing baseline competencies that are necessary to run a secure and reliable operation, taking an inventory of skills, identifying gaps in skills, and addressing the skill deficiencies either by hiring appropriate personnel or by providing training to current employees.

III. CONCLUSION

An effective CIP compliance program that is properly executed requires an appropriate amount of technical expertise, senior management involvement, and a sense of ownership on the part of employees responsible for executing CIP compliance procedures. Once an entity develops a coordinated, effective compliance program, with input from senior management and others responsible for executing the program, the entity needs to consistently execute this coordinated compliance program throughout the entity. If any of these pieces are missing, an entity may encounter significant struggles in maintaining compliance with the CIP Reliability Standards and further ensuring that its system is operating in a secure state.