Opening Remarks by
Patrick C. Miller, Managing Partner, The Anfield Group

Federal Energy Regulatory Commission Technical Conference on
Critical Infrastructure Protection Issues Identified in Order No. 791

NIST Frameworks Discussion
April 29, 2014

Good afternoon. I would like to offer my sincere thanks to the Commission for holding this technical conference on the subject of the NIST Cyber Security Framework (CSF) as it relates to the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards. It is an honor to be on such an esteemed panel with my industry colleagues and I am pleased to appear here to today to discuss the importance of cybersecurity for the electricity subsector.

My name is Patrick Miller, and I am a Managing Partner at The Anfield Group. The views I will express today are based on over 25 years in various technology and infrastructure-related positions, but most importantly, 15 years of direct security experience in the electric power industry through my roles as a former utility security employee; former manager of audits and investigations for the Western Electricity Coordinating Council (WECC), the largest of the Regional Entities charged with monitoring and enforcement of the NERC CIP standards; founder of EnergySec, the oldest grass-roots non-profit training and information sharing organization for security in our subsector; and advisor to many utilities and vendors in the electric power sector as well as local, state, federal and international agencies. I am one of the few who have drafted, implemented, audited, enforced and advised on the NERC CIP standards.

- - - - -

Critical infrastructure organizations have civic, fiscal and moral duties to protect their systems from attack. They should be held accountable for these responsibilities. However, adding overly prescriptive regulation may have the effect of introducing a competing prerogative: the fiduciary duty to avoid legal penalty for non-compliance. This has the potential to divert resources from real, tangible security and reliability improvement efforts. The unfortunate reality is that we presently fear the auditor more than the attacker.

But make no mistake - the electric power industry is not waiting for regulation or new frameworks to secure their environments.

Successfully responding to and preparing for threats and risks and rapidly restoring the grid to a safe state of operation are industry-wide responsibilities that are taken very seriously. This is evidenced by the fact that even though the North American power grid is by far the largest, most complex system ever built by humans, it is also the most reliable. Our utilities already respond to catastrophe with the skill and aplomb that only comes from years of experience and refined maturity. They do this every day and they do it very well. Cybersecurity is another important variable in their risk landscape, but it doesn't significantly change the overall risk management approach. Like all other risk mitigation efforts, cybersecurity protections should support the mission of delivering safe, reliable power to the consumer.

There are many perspectives and positions on security for our industry. Some are polarizing. Some are complimentary. There is no shortage of ideas and opinions on how we can all collectively or separately advance security within the subsector. However, each approach comes with risk and reward. The challenge is to find the most appropriate mix that results in raising the security bar with the lowest degree of unintended consequences.

Legislation and regulation are certainly necessary to move us forward. They form the structure and frame of reference for all of the various parties attempting to manage security risk for the industry. I am in favor of certain types of regulation, however as a practitioner in this field I caution that regulation can be a difficult vehicle through which to effect a net-positive change on security – cybersecurity in particular. Many of the best-intended approaches are challenged to achieve their expected outcome.

The NIST CSF has been introduced as a voluntary approach. Note that many believe this is only preliminary until it can gain enough acceptance and replace the existing regulations. It is effectively seen as "de facto" or "quasi" regulation already. It is discussed in expert forums as though it is regulation. It is being requested through mandatory oversight venues such as State Public Utility Commissions and Regional Entities under NERC. Whether voluntary or not, the genie is out of the bottle.

While in favor of some regulation to establish minimum bars and "guard rails," I will always contend that hackers are faster than laws. The existing body of legal precedent[1] on the subject of cybersecurity hasn't stopped the flood of ever-increasing cybersecurity issues. After so many billions spent on "required" security, at some point we need to question whether our legislative, regulatory and enforcement structures are the only solution.

To be very clear, I'm not implying that we should throw out all regulation. Rather, we should look at places where regulation will work and where it won't – where is has the highest value and where it doesn't.

- - - - -

It is important for any participant in North American power grid to have a firm grasp on their operations environment. When a problem occurs, knowing who owns, who operates and who supports that system is essential to rapid detection, isolation and response. These are the core elements of "resilience." Currently, no inventory is required within the CIP Standards, particularly for the Low impact systems. This makes knowing your environment difficult.

Organizations should be fully aware of the vulnerabilities within their portion of the system. It also important to know the threat actors, their motivations and activation triggers. Additionally, it is important to know the potential impacts, should a threat actor choose to exploit those vulnerabilities. The CIP version 5 standard is effectively silent on knowledge

[1] Federal Laws Relating to Cybersecurity: Discussion of Proposed Revisions, Eric A. Fischer, Senior Specialist in Science and Technology December 22, 2011

of the threat landscape and security situational awareness. It does speak to vulnerability management, requiring utilities to manage configuration baselines and track, evaluate and install patches for many systems, at least those that are updateable and where a patching source exists. Impact is managed through methods of detection followed by incident response and disaster recovery. However these requirements vary as they are related to the High, Medium and Low impact categories. It is important to note that there are exclusions and allowances for lower risk and legacy systems.

The DOE Risk Management Process and the NIST Cybersecurity Framework both address threat, vulnerability and impact, arguably in greater detail than the NERC CIP standards. In many cases, they both account for the subtle differences between Information Technology (IT) methods and Operational Technology (OT) methods. The NERC CIP standards apply many of the same methods to both IT and OT, with an allowance for technical infeasibility on legacy or ICS equipment.

- - - - -

During the CIP version 1 implementation phase, the concept of the Risk Based Assessment Methodology (RBAM) was used. This model allowed the utilities to decide which facilities (e.g. control centers, transmission substations, generation plants) are critical and which aren't. The official guidance at the time suggested removing the concept of probability from the traditional risk equation (risk = probability x impact), resulting in something more closely resembling an impact assessment.

Everyone was left to choose his or her specific direction in CIP version 1. The degree of inconsistency was significant. This inconsistency ultimately led to the creation of the "Bright Line Criteria" within Attachment 1 in CIP version 4 as an attempt to get a more consistent application of the process. The Bright Line Criteria used an engineering-based approach, leaning heavily on the NERC Glossary of Terms. CIP version 5 also uses a set of Bright Line Criteria but changed the model such that all facilities were critical to some extent, and introduced the concept of High, Medium and Low risk impact elements.

I would argue that none of the aforementioned approaches solved the problem. When the binary critical approach was used in CIP versions 1-4, many scrambled to exercise the flexibilities around routable protocols, engineering studies, etc. They didn't do this to intentionally make their system less reliable. They did it because of the cost associated with being critical. Now, in version 5, a similar approach is being taken around finding the "right" position within the high, medium and low categories. Again, cost being the primary motivator. In many cases, the cost of compliance outweighs the cost of the penalties for noncompliance. These facts are proof that you can prescribe action, but you can't prescribe attitude.

The biggest influences contributing to confusion were, and are still, cost and culture. Security costs money. Security affects culture. I haven't met a utility yet that wouldn't readily apply every reasonable security best practice if they could afford it – and as long as it didn’t impact reliability. Utility culture is steeped in reliability. It is safe to say that when security supports reliability, utility culture will respond very positively.

The challenge is getting the engineering mindset to mesh well with the security mindset. Engineering deals with physics. It is about trying to manage mother nature. Mother nature may be harsh, but she’s not malicious. Conversely, security deals with malice. When we merge these disciplines, we end up with a better picture of what is critical and why we should spend the money necessary to protect it.

Early in the CIP version 1 discussions, an astute colleague of mine with a long background in both engineering and security suggested looking at the problem from a different perspective. His “methodology” for determining criticality was very simple. He stated: “If you would mind your adversaries controlling that facility, system or cyber asset, then it’s probably worth protecting.”

However, It simply isn’t feasible to protect everything to the same degree. Some elements of the grid need more protection than others. Where we can’t protect and prevent (or it may be infeasible) the most effective proven options are detection and response. What isn’t found in the CIP standards is the balance of detection and response for the Low impact category.

- - - - -

Comparing the CIP Standards to the NIST CSF and DOE RMP, and asking which one is better may not be the most effective approach. Although we are more than 10 years down this road, we still aren’t sure if this direction is the best way to get to our destination. We need a better understanding that we are actually moving the security needle and not impacting reliability at the same time.

Currently, we are trying to manage risk through regulation and voluntary incentive. In order for risk management to be effective, regardless of the drivers, we must understand the risks enough to manage them. Understanding requires analysis. Analysis requires data and data requires measurement. It has been said, “you can’t manage what you don’t measure.”

The risk management challenge begins with measurement and collecting data for analysis. Some good models exist for security metrics and telemetry. A very good example can be found in the aviation oversight and reporting relationship between the Federal Aviation Administration (FAA) and the National Aeronautics and Space Administration (NASA).

We have very little cybersecurity actuarial data in this sector. Understanding that electric power is without question the most critical of the critical infrastructures, it is easy to fall into the trap that this type of information is just too sensitive to collect. We’ve gathered sensitive data to improve and advance healthcare, enhance aviation and automobile safety, and even manage fraud in complex financial systems. Without actuarial data from which to make informed and intelligent decisions, we are essentially guessing and hoping we get it right. Neither the CIP Standards nor the NIST CSF nor the DOE RMP speak to mandatory or voluntary methods to obtain this actuarial data. The industry deserves to know if the money we are spending on these requirements is actually providing security value and improved reliability and resilience.

I would contend that few in this world are better at telemetry than electric utilities. We understand measurement and instrumentation better than most. Putting this experience together with hybrid analysis from both the engineering and security disciplines may help the industry advance beyond the "guess" and begin to illuminate the areas of security benefit provided by current regulation as well as any potential gaps.

Whichever path we choose, or which path is chosen for us, we should endeavor to maintain consistency. Through consistency, measurement and constructive dialogue we will be able to have a better understanding of whether or not we are making a difference.

Thank you again for your time and I look forward to the discussion today.