Setting Standards for Excellence

KYLE PITSOR
Vice President, Government Relations

April 8, 2013

SUBMITTED VIA EMAIL: cyberframework@nist.gov

Ms. Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

RE: Developing a Framework to Improve Critical Infrastructure Cybersecurity (Docket Number 130208119–3119–01)

Dear Ms. Honeycutt:

NEMA is the association of electrical equipment and medical imaging manufacturers, founded in 1926 and headquartered in Arlington, Virginia. Its member companies manufacture a diverse set of products including power transmission and distribution equipment, lighting systems, factory automation and control systems, and medical diagnostic imaging systems. Worldwide annual sales of NEMA-scope products exceed $120 billion. These comments are submitted on behalf of the NEMA Smart Grid Council.

NEMA believes protection from and the ability to respond to cybersecurity events are critical to the Smart Grid. Cybersecurity policies must provide a common risk-based approach that gives manufacturers, utilities, and grid operators the flexibility to respond quickly and decisively.

Since its founding, one of NEMA's core functions has been to develop and promote standardization in the electrical sector. NEMA is an ANSI-accredited standards development organization with a history of national and international leadership.

Executive Order 13636, *Improving Critical Infrastructure Cybersecurity,* has charged the National Institute of Standards and Technology (NIST) with developing a framework "to lead the development of a framework to reduce cyber risks to critical infrastructure." Further,

> The Cybersecurity Framework shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. The Cybersecurity Framework shall incorporate voluntary consensus standards and industry best practices to the fullest extent possible. The Cybersecurity Framework shall be consistent with voluntary international standards when such international standards will advance the objectives of this order, and shall meet the requirements of the National Institute of Standards and Technology Act, as amended (15 U.S.C. 271 et seq.), the National Technology Transfer and Advancement Act of 1995 (Public Law 104-113), and OMB Circular A-119, as revised.

NIST has proven itself to be an organization that is capable of serving as the venue for industry and government to come together to discuss and develop standards. NIST's leadership of the Smart Grid Interoperability Panel (SGIP) over the past view years is a testament to this capability.

As NIST embarks on developing a framework to address cybersecurity, NEMA encourages NIST to use the lessons it has learned through the SGIP experience.

Performance-based objectives and technology neutrality

A hallmark of the Cybersecurity Framework should be technology neutrality. Government endorsement of specific cybersecurity practices and technologies would be counterproductive to the protection of critical infrastructure by limiting the number of approaches owners of critical infrastructure may consider and by placing a chilling effect on innovation, which is key to staying ahead of the cyber threat.

Indeed, the Cybersecurity Framework should help to establish performance-based objectives and allow the private sector to determine the best way to achieve them.

Compatibility with existing electrical grid

The electrical grid has been called the world's largest machine. The equipment comprising the grid has been manufactured and installed over a century and as such exists at various levels of technological maturity and standardization. Despite the significance of the cyber threat, the country is not building a new electrical grid from the ground up.

Therefore, the Cybersecurity Framework should give consideration to the enormous amount of legacy equipment that makes up our electrical grid. Any framework must be compatible with the installed base of existing systems.

Architecture: Segmentation and layering

The electrical grid is a collection of contiguous, interconnected physical devices from the point where electricity is generated to the point of use. A segment of the grid is any set of elements for which the electricity supply can be controlled as a unit. This may be a single building such as an office high-rise, a group of related buildings such as an educational or industrial campus, or a collection of buildings or homes such as a military base or a residential neighborhood.

In order to control the cost of deployment, government needs to consider the overall security architecture of its decisions. The ability to isolate security issues and insulate core grid functionality from their effects is as important as the strength of the security measure.

A layer is the application of a security measure in the cybersecurity architecture. For example, the first layer of security is the physical connection to a device in the Smart Grid. Another layer could be a login server to authenticate any user that is trying to issue commands to Smart Grid devices. Encryption is yet another layer, and so on. Having a layered security architecture

implies that multiple security measures could be applied to any connection to the Smart Grid.

The aspect of security layering needs to be considered during creation of the framework. Individual security measures should not be considered in a vacuum, but rather in the context of how they contribute to the overall security architecture of the system. It would be important to define rules and guidelines for the levels of layered security required as a function of the criticality of a device, its functions, the impact on the surrounding segments of the grid, etc.

Integrity and security of the supply chain

NEMA member companies agree that first and foremost, security must be part of the design consideration for any Smart Grid component (and its corresponding interactions with other grid elements) from its inception.

NEMA has identified four key areas in the supply-chain framework where cybersecurity plays a role: technical standards, procurement, manufacturing, and on-going assurance. The process starts with technical standards. Specific cybersecurity aspects need to be included in these documents. Corresponding cybersecurity language would then be embedded in subsequent procurement documents. This allows for more up front disclosure and sharing of information between purchaser and supplier. Manufacturers will need to validate compliance with their product designs. Finally, on-going assurance is need once these products arrive at the purchaser's docks (i.e. tamper-resistant packaging and designs, software/firmware assurance, security keys, and post-delivery on-site inspection).

By focusing on the integrity of the supply chain, NEMA member companies can work to mitigate vulnerabilities.

Sustainability

To maximize the effectiveness of the Cybersecurity Framework, we must ensure that the result is compatible with utility practices, now and in the future, so that owners of critical infrastructure can sustain a high level of cyber protection on an ongoing basis.

Hardware-based standards for cybersecurity must be designed appropriately for the operating environment (including the method of deployment, administration) and any operational considerations (such as weather for outdoor devices). They must also integrate with widely-accepted management systems and practices associated with the electrical industry.

As with hardware-based standards, software solutions in cybersecurity need to be compatible with widely-accepted management systems and practices. Both interoperability and sustainability need to be factored into the features of any standards developed or adopted for software systems.

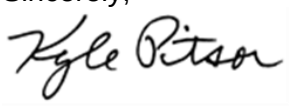
Limitations of the communications associated with the electrical grid need to be part of the design criteria for cybersecurity standards. Unlike the internet, the electrical grid was not

designed as a communications network and therefore cannot support heavy message loads; long-haul distances with limited access to bandwidth will be the norm in many cases.

For the development of any standard in the cybersecurity arena, the concept of how that standard will be supported after deployment needs to be considered. In a distributed operating environment with literally millions of nodes, manual maintenance is not a viable option. The application of a security standard as a component of a larger security architecture needs to permit remote administration.

On behalf of its Smart Grid Council, NEMA appreciates the opportunity to provide these comments on the development of a Cybersecurity Framework. NEMA looks forward to continuing to provide the manufacturers' perspective on policies that will have a significant impact on the electrical grid and its supply chain.

Sincerely,



Kyle Pitsor,
Vice President, Government Relations