NEMA

Setting Standards for Excellence

KYLE PITSOR
Vice President, Government Relations

December 13, 2013

Mr. Adam Sedgewick
Information Technology Laboratory
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-8930

RE: Preliminary Cybersecurity Framework Comments

Dear Mr. Sedgewick:

Thank you for providing us the opportunity to submit comments in response to the National Institute of Standards and Technologies' (NIST) Preliminary Cybersecurity Framework ("the Framework").

The National Electrical Manufacturers Association (NEMA) is the association of electrical equipment and medical imaging manufacturers, founded in 1926 and headquartered in Arlington, Virginia. Its 400-plus 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. The U.S. electroindustry accounts for more than 7,000 manufacturing facilities, nearly 400,000 workers, and over $100 billion in total U.S. shipments.

These comments reflect the viewpoints of NEMA members including members of the Medical Imaging & Technology Alliance (MITA), a division of NEMA.

NEMA believes that the Framework contains logical key principles that are risk-based and capable of keeping pace with evolving threats. It provides high-level guidance, which appears to be the goal. The Framework is not very specific regarding outcomes and tools, leaving that to supporting standards. Some examples of its lack of specificity include the lack of a process for developing more secure products, and no method for addressing security on existing products in the market.

The Framework does not provide much direction on how to define the gap between the current state and the desired target state of a specific cybersecurity activity. This is only done conceptually and the Framework leaves it to the individual organizations to create their own profile tiers.

NEMA is supportive of the general description of terms, activities, maturity levels, and references toward implementing cybersecurity processes at an enterprise level, as different markets have variable cybersecurity requirements, ranging from critical infrastructure to public systems that do not require a lot of security. This broad Framework can be seen as a useful reference when organizations implement cybersecurity-related processes, particularly since there are no onerous direct technical requirements.

However, the Framework is just one component of a predictive cybersecurity process that should also include:

- Effective information sharing between government and industry partners, including classified information, in real time;

- Information sharing liability protection, which will safeguard companies who participate in these activities in good faith; and

- Appropriate incentives for companies to develop proactive, preventive, and predictive capabilities for cyber defense.

NEMA offers the following comments on particular portions of and specific issues in the Framework.

1. The Framework should better clarify the roles and responsibilities of owners and operators of critical infrastructure from the roles and responsibilities of the technology suppliers who manufacture the products composing critical infrastructure. There are instances in the Framework where delineation between these two could be misinterpreted.

   As an example, in Section 3.3 the Framework discusses providing a common language for critical infrastructure owners and operators to communicate requirements among interdependent partners responsible for the delivery of essential critical infrastructure services. A technology supplier could be considered an interdependent partner. Yet, in the introduction a statement reads, “The critical infrastructure community includes public and private owners and operators, and other supporting entities that play a role in securing the Nation’s infrastructure.” The term “other supporting entities” could be interpreted to mean technology suppliers. This would seem to contradict what is mentioned later in the document.

2. Consideration should be given to organizations’ and entities’ current cybersecurity risk management processes and procedures. It is mentioned in the introduction that the Framework complements—and does not replace—an organization’s existing business or cybersecurity risk management process and cybersecurity program. It also states that an organization can use its own current processes and leverage the Framework to identify opportunities to improve an organization’s management of cybersecurity risk.

   What if an organization’s current processes and procedures are deemed more than capable of addressing cybersecurity risks? Many NEMA member companies already have very robust cybersecurity risk management processes and procedures in place. In addition, these select companies may already have formally adopted existing ISO or IEC security standards and certifications that satisfy the requirements of the Framework. If an organization can demonstrate this either via self-certification or third-party certification, can it be considered to have adopted the Framework? Since most organizations conduct these types of assessments as matters of business, it would be of value for the government to recognize and accept these attestations as a measure of an organization’s cybersecurity/information security maturity.

3. NIST should consider having the Framework reference the Building Security In Maturity Model (BSIMM) as a de-facto measurement model in its informative reference list.

4. NIST should consider having the Framework reference healthcare-specific standards such as ISO/IEC-80001.

5. The Framework should promote a continuous improvement process. Not until the Respond and Recover phase is there a reference about improvement and even then it does not take into account explicit lessons learned. Nor is there an acknowledgement that when there are organizational changes, such as a new acquisition or a major change in assets, that the organization should determine if the current security posture is still adequate.

6. The Framework needs to emphasize the importance of a skilled cybersecurity workforce to raise the level of technical skills of those who operate critical infrastructure. NIST should consider including an informative reference list which contains cybersecurity certifications and corresponding summaries of competencies that each certification provides to help organizations understand their current and future needs.

7. The Framework is vague on mapping and harmonization of global standards, laws, and regulations. A list of informative references to existing standards is included in the Framework in Table 1. This list of standards does not mention all existing international efforts. We are concerned that this list may be mistaken to be a checklist of a reference to mandatory standards. NEMA requests that NIST make it clear that other standards may be applicable. NEMA further requests that NIST show support for the selection of the referenced standards and how other standards may be selected for inclusion.

8. We believe privacy and cybersecurity go hand in hand. As such, we applaud NIST's willingness to address privacy issues in the Framework. Although the inclusion of privacy standards in the Framework is important, a privacy methodology that includes open-ended and burdensome mandates could serve to discourage organizations from adopting the voluntary Framework. NEMA urges NIST to review and revise the Framework's privacy methodology (Appendix B) to ensure the methodology is narrowly focused to reflect consensus private sector practices relating to privacy. By including an appropriately tailored privacy methodology as part of the Framework, NIST will encourage the adoption of the Framework and allow an organization to complement its cybersecurity program with a privacy program that addresses privacy issues directly implicated by the organization's approach to cybersecurity.

9. The Framework tiers, which try to make this into a capability maturity model, are almost all listed as passive, not active. This suggests that one can move between tiers and have no impact on actual risk.

10. The Framework fails to address one of the largest gaps in existing standards, guidance, and best practices, which is threat management. That is a key component in risk management that needs more guidance.

11. This Framework does not adequately address measuring and reporting of risk. If the intention of this Framework is to improve our ability to effectively manage risk in critical infrastructure, how can we know whether it is effective at the micro or macro level?

12. NEMA is concerned with how this Framework will work once it is implemented and how its success will be measured. It lacks specific Adoption/Conformity guidelines. Such guidelines would provide organizations with a standard process to assess the maturity of its implementation of the Framework Functions and Profiles. Organizations are invited to "self-assess" compliance and assign current and target tiers, but there are no objective criteria for the assessments, thus no common language between organizations. It is also not immediately clear the role of the Department of Homeland Security (DHS) and its voluntary program for Framework adoption. There also remains the possibility that other government agencies will step in and provide conflicting guidance on the Framework's implementation. NEMA would appreciate guidance on this matter.

NEMA thanks you for the opportunity to provide this information. Should you have further questions, please contact Steve Griffith, NEMA Cybersecurity Program Manager, at steve.griffith@nema.org or 703.841.3297.

Respectfully,

Kyle Pitsor

Kyle Pitsor

Vice President, Government Relations