Setting Standards for Excellence

KYLE PITSOR
Vice President, Government Relations

April 29, 2013

SUBMITTED VIA EMAIL: cyberincentives@ntia.doc.gov

Mr. Alfred Lee
Office of Policy Analysis and Development
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4725
Washington, DC 20230

RE: Incentives to Adopt Improved Cybersecurity Practices (Docket Number 130206115–3115–01)

Dear Mr. Lee:

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.

NEMA member companies supply products and technologies to a wide variety of end users, many of whom may be considered owners of critical infrastructure as identified by the Department of Homeland Security per Executive Order 13636.

NEMA members' customers demand performance from their products and one performance characteristic gaining increased attention is cybersecurity; therefore managing cybersecurity risks on behalf of customers is part of NEMA members' businesses and a constant consideration in their daily work.

We thank the National Institutes of Standards and Technology (NIST) for the opportunity to provide input for the "establishment of a set of incentives to promote participation in the [Department of Homeland Security's] Program" (the Program) designed to encourage adoption of the Cybersecurity Framework being developed by NIST as directed by the Executive Order.

First and foremost, NEMA encourages NIST to consult owners of critical infrastructure for guidance on incentives that would be most effective in encouraging them to participate in the Program.

NEMA notes, however, that because the Program is designed to encourage adoption of an as yet unpublished Cybersecurity Framework, comments on necessary incentives will not have the benefit of a full understanding of what adoption of the Cybersecurity Framework entails.

The Notice of Inquiry also requests comment from non-owners of critical infrastructure. It is NEMA's expectation that by and large, suppliers of equipment and technology would fall into this category.

Supply Chain Participation

Incentives should be geared toward encouraging supply chain participants to take part in the Program.

The security of critical infrastructure is inextricably linked to the security of the products that comprise it. NEMA member companies agree that first and foremost, security must be part of the design consideration for any component at its inception.

NEMA has identified four key areas in the supply-chain framework where cybersecurity plays a role: technical standards, procurement, manufacturing, and ongoing 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, ongoing assurance is needed 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).

Failing to include supply chain ignores a critical piece of the cybersecurity puzzle.

Broad Accessibility

Incentives should be constructed so that they are accessible by the full range of interested parties.

If incentives are too narrowly drawn, they will leave out key players or entire sectors or subsectors which may represent owners and non-owners of critical infrastructure. A robust Program will encourage participation by all stakeholders by offering incentives that are broadly beneficial.

International Coordination

The electrical manufacturing industry is a global one. A significant portion of products and technologies comprising U.S. critical infrastructure are manufactured outside the U.S. Conversely, U.S. manufacturers sell their products and technologies in the global marketplace.

Many governments are moving rapidly to address the cyberthreat through laws and regulations.

Incentives for non-owners of critical infrastructure should be structured in such a way that acknowledges cybersecurity policy development in other countries, so as not to place an unnecessary burden on U.S. manufacturers who may be interested in participating in such a Program, but who are also participating in cybersecurity regimes in other countries.

Incentive Structures

Standards Development
In much the same way that manufacturers must be mindful of foreign governments' cybersecurity policies in the development of their products and technologies, NEMA members are actively engaged in national and international standards through a number of standards development organizations.

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.

Incentives to participate in a Program that includes the application of standards should contemplate the value of international harmonization of standards and offer support for U.S. leadership and international cooperation in standards activities. Cyberattacks do not respect international borders so ensuring that cybersecurity standards are robust internationally is critical.

Liability Protection
NEMA members are committed to helping the U.S. defend against the cyberthreat. A key attribute to this partnership is a sense of cooperation in the face of a common threat.

To truly encourage non-owners of critical infrastructure to participate in the Program, reasonable and relevant liability protection should be provided to Program participants.

Industry Consortia
Incentives could also be structured to promote collaboration among sectors of the economy that have shared responsibility when it comes to product development. Because the cyberthreat stems in part from information and communication technologies being incorporated into hardware, a collaborative effort between the IT sector and NEMA manufacturers, for instance, would improve the supply chain's response to the cyber vulnerabilities.

Research and Development
NEMA believes research and development in the cybersecurity arena is a critical component of a complete cybersecurity policy. Government support of private sector R&D could be a tool that would incent industry actors to participate in the Program.

NEMA appreciates the opportunity to provide these comments on the development of a set of incentives to encourage participation in the Program. NEMA looks forward to continuing to provide the manufacturers' perspective on policies that will have a significant impact on critical infrastructure and its supply chain.

Sincerely,

Kyle Pitsor
Vice President, Government Relations