Cybersecurity Policy Principles

Protecting electrical and medical imaging products and systems from unauthorized access without compromising functionality is an evolving challenge. NEMA Members make products that are used in critical infrastructure around the world, and they manufacture increasingly secure products for their customers to reduce the risk that these critical systems will be compromised.

The responsibility for protecting our nation's critical infrastructure from cyberattack is shared by multiple stakeholders, including the federal government, private industry, and end-users. NEMA Members believe in the following cybersecurity policy principles:

- **Shared Responsibility**

  Effectively defending critical infrastructure sectors against cyber threats requires a holistic collaborative approach between senior individuals and designated decision makers within government, private entity owners, systems operators and integrators, and product end-users. All must work collectively and be determined to advance established, scalable, and practical cybersecurity standards and strategies.

- **Harmonization of Industry-Developed Standards**

  Policymakers within the United States should incentivize the adoption of industry-developed, technology-neutral cybersecurity standards and best-practices. Furthermore, they should continuously collaborate with the electroindustry to ensure the harmonization of standards in order to enhance security and drive innovation.

- **Information Sharing**

  Public and private sector collaboration on cybersecurity creates a foundation of trust and mutual understanding which is necessary to implement effective policies. Government should incentivize reasonable and voluntary two-way information sharing between itself and the private sector, including entities within critical infrastructure sectors.

  When information is required by government to be submitted, such as in the aftermath of a cyber-attack, demands must not erode the principles of shared responsibility and collaboration.

- **Research and Development**

  The federal government should fund cybersecurity research and development activities at the National Institute of Standards and Technology, Department of Energy, Department of Homeland Security, and other relevant agencies.

- **Education and Workforce Development**

  The diversity of the electroindustry requires proactive advocacy to educate policymakers on the various cybersecurity standards its companies use. They need to be made aware of the distinction between information technology and operation technology, what industry-developed cybersecurity standards currently exist, and what legal definitions and vernacular on cybersecurity are widely accepted.

  The exponential growth in connectivity and digitization requires that the electroindustry have an educated and qualified workforce to ensure industry-developed cybersecurity standards are integrated into products and applied with effect. Dedicated cybersecurity courses, including disciplines focused on operational technology, should be offered in school curricula—as degree courses in universities, professional education, and trainings—in order to better defend critical infrastructure. Public investment and incentives are necessary to educate and develop a cybersecurity-savvy workforce.

Contact: *Peter Ferrell: Manager, Connectivity and Data Policy: 703-841-3280 | peter.ferrell@nema.org*

Updated January 2022.