Cybersecurity Policy Priorities (Appendix)

The following priorities are rooted in NEMA's Cybersecurity Policy Principles and are meant to serve as the charge for the organization's advocacy in this area. These principles should be reviewed annually by the Cybersecurity Council and amended as necessary.

Shared Responsibility

- Congress should provide dedicated agencies, including the Cybersecurity and Infrastructure Security Agency (CISA), with appropriate resources which further the voluntary collaborative relationship between government and the private sector on cybersecurity.

- Collaboration between government and private sectors should be constructive and mutual. Critical infrastructure sector working groups designated by CISA should contain individuals who are knowledgeable in cybersecurity policy and dedicated to developing actionable outcomes. Engagement without clear objectives or desired outcomes should be discouraged.

Harmonization of Industry-Developed Standards

- Government should enact policies that encourage the adoption of electroindustry-endorsed cybersecurity standards. These include, but are not limited to, the NIST Cybersecurity Framework, ISO 27000 Series of Standards, IEC 62443 Series of Standards, and NEMA CPSP Series of Standards. The adoption of one standard should not exclude others.

- Legislatures should incentivize electroindustry cybersecurity standard adoption by providing "safe harbor" from liability. Enactment of a federal policy is preferred.

- Breach notification laws should be harmonized throughout the United States through the enactment of a federal policy.

- Through collaboration with electroindustry partners and government agencies, establish voluntary, non-burdensome, and understandable cybersecurity postures for IoT devices and product development.

- Cybersecurity labeling schemes should be voluntary, industry-developed, tiered, and provide liability protections.

Information Sharing

- Entities required to submit information to a government agency should be granted anonymity and protections from legal liability.

- Reporting obligations should be limited to the entity that is a victim of a cyberattack. Vendors and non-affected third parties should be exempt from reporting. Additionally:
    - A reporting timeline of no less than 72 hours should be established for a victim to analyze the extent of an attack and to ensure accurate and actionable information is being shared with authorities.
    - Objective baselines should designate when a mandatory reporting timeline officially beings.
    - Required information should be limited in scope and focus only on what is pertinent to the cyberattack itself.
    - Reporting should only apply to an entity that experienced a cyberattack within the jurisdiction of the United States.
- Since cybersecurity standards vary by industry sector, government should collaborate with industry to create acceptable definitions of a "cyber incident." Additionally, such definitions should be uniform throughout government.
- Every effort should be made to preserve the open and voluntary collaboration and exchange of information between government and the private sector on cybersecurity related matters.

Research and Development

- NEMA should advocate for grant funding which promotes the adoption of electroindustry-endorsed cybersecurity standards. These include, but are not limited to, the NIST Cybersecurity Framework, ISO 27000 Series of Standards, IEC 62443 Series of Standards, and NEMA CPSP Series of Standards.

Education and Workforce Development

- Standard and technology-neutral grant funding and scholarships should be made available to students seeking an education in cybersecurity. Any dedicated funding should support both operational and informational technology cybersecurity disciplines.
- Electroindustry-focused cybersecurity apprenticeships or similarly credentialed educational programs should be established with nationwide and/or international recognition.
- Government should incentivize "bug-bounty," "capture the flag," and other stress-testing programs to help private industry bolster their cybersecurity posture.

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

Updated January 2022.