



November 14, 2022

Mr. Todd Klessman
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
245 Murray Lane
Washington, DC 20528-0380

RE: Docket ID: CISA-2022-0010 | Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022

Mr. Klessman:

The National Electrical Manufacturers Association (NEMA) welcomes the opportunity to submit comments in response to the Cybersecurity and Infrastructure Security Agency's (CISA) request for information (RFI) on various elements related to the implementation of the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA). We are the leading U.S. trade group representing nearly 325 electrical equipment and medical imaging manufacturers that make safe, reliable, and efficient products and systems. A limited assortment of NEMA members manufacturer products and systems considered crucial to the operations of other critical infrastructure sectors. Our comments are meant to help guide CISA as it seeks to properly implement CIRCIA so that incident reporting can help harden critical infrastructure sectors against cyber threats and attacks. They also serve as a complement to NEMA's oral statements made during two listening sessions regarding this topic in Chicago, IL (October 5, 2022) and Washington, D.C. (October 19, 2022).

(1) Definitions, Criteria, and Scope of Regulatory Coverage

a. The meaning of “covered entity,” consistent with the definition provided in section 2240(5) of the Homeland Security Act of 2002 (as amended), taking into consideration the factors listed in section 2242(c)(1).

CIRCIA specifies a “covered entity” as being an entity in a critical infrastructure sector as identified in Presidential Policy Directive 21 (PPD 21). Issued by the Obama Administration in 2013¹, PPD 21 has long provided useful guidance to the private sector by helping it understand which industries and operations are within the government's scope of “critical infrastructure.” The directive lists 16 economic sectors, which includes the Critical Manufacturing Sector (CMS), and designates a sector risk management agency (SRMA) to be both a partner with and liaison for the entities within the sector. CISA is the designated SRMA for the CMS.

¹ <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>

Currently, CISA has specified four core industries that fall under the auspices of the CMS, industries that are considered “crucial to the economic prosperity and continuity of the United States.”² NEMA’s membership includes companies which fall primarily under two of these four core industries, namely the *Machinery Industry* and the *Electrical Equipment, Appliance, and Component Industry*. Within these four industries, CISA distinguishes CMS members as being companies or organizations which are directly involved in the production of certain identified products.

This distinction is important because it clarifies CMS members to what they manufacture rather than just being engaged in manufacturing generally. For the Machinery Industry, the product types CISA considers critical include engines, turbines, and power transmission equipment. For the Electrical Equipment, Appliance, and Component Industry, critical product types include electric motors, transformers, and generators. These products have been recognized by CISA as vital to the security and functionality of entities within other critical infrastructure sectors. NEMA feels that there is no immediate reason or justification to expand the list of products within the four core CMS industries.

Therefore, in defining “covered entity,” **NEMA recommends that CISA (1) maintain the four core CMS industries already recognized by the agency, and (2) only apply the definition to those manufacturers that produce the specific product types clearly identified within each.** By following these recommendations, CISA will greatly help clarify which manufacturing companies the final rule will apply to.

Furthermore, manufacturers of products used by entities of other PPD 21-identified sectors should not be classified as a “covered entity” if their products are not clearly identified as being critical to their security or functionality. Owners and operators of critical infrastructure procure and apply various products in myriad ways, depending on available resources and their end goals. For example, within the Commercial Facilities Sector, an owner/operator of a mall may purchase and customize various products made by electromanufacturers, such as building management systems, lighting products and control systems, and fire and safety control systems. To maximize their potential benefits and usefulness, most of these products can be fully integrated and interconnected.

However, it is the ultimate responsibility of an owner/operator to ensure that these products are secure from cyber threats. A product can be designed to be secure against a given standard, but it is how it is deployed which will determine its level of risk. A manufacturer may not or cannot know how their product will be governed or manipulated. Therefore, **a “covered entity” should be limited to the owner and operator of a specified critical infrastructure and not be expanded to include supply chain vendors or partners.**

² <https://www.cisa.gov/critical-manufacturing-sector>

c. The meaning of “covered cyber incident,” consistent with the definition provided in section 2240(4), taking into account the requirements, considerations, and exclusions in section 2242(c)(2)(A), (B), and (C), respectively. Additionally, the extent to which the definition of “covered cyber incident” under CIRCIA is similar to or different from the definition used to describe cyber incidents that must be reported under other existing federal regulatory programs.

&

e. The meaning of “substantial cyber incident.”

In defining “covered cyber incident,” the CIRCIA text refers to a “substantial cyber incident experienced by a covered entity that satisfies the definition and criteria established by the Director in the final rule issued pursuant to section 2242(b).”³ The law, however, neither defines the term “substantial,” nor does Section 2240 of the Homeland Security Act of 2022 (as amended) on which many authorities of CIRCIA are rooted in. In fact, “substantial” has never been defined in law or policy. Rather, a “significant cyber incident” currently exists in the U.S. code and is defined in Presidential Policy Directive 41, issued in 2016.^{4 5}

The RFI seeks to guide CISA to establish a “substantial” standard in order for it to be applied to cyber incidents which must be reported via the law. **NEMA strongly encourages CISA to formulate a definition which is as similar as possible to “significant cyber incident,” notably incidents which do or are likely to result in real harm.** Many cybersecurity frameworks and assessment standards, including those detailed below, are built upon the foundation of a significant standard. In crafting a definition which goes beyond what industries have long used as a baseline could seriously undermine many of these models.

The electroindustry manufactures products using sophisticated and unique techniques and processes. Especially for those CMS industries which produce critical components, their production methods can be extremely intricate, customized, and often proprietary. In drafting a practical definition for “covered cyber incident,” CISA needs to take into consideration the complexities of each critical infrastructure sector since the cybersecurity standards and approaches for entities will vary greatly based on their operational environment and goals.

CISA already recognizes that cybersecurity cannot be and should not be considered in general terms. The National Cyber Incident Scoring System (NCISS) was developed to allow CISA and other agencies the ability to “assess risk while accommodating a diverse set of private critical infrastructure asset owners and operators” and “provide a repeatable and consistent mechanism for estimating the risk of an incident in this context.”⁶ This system is intended to help CISA weigh the severity of a cyber incident against an entity. By using various criteria and metrics, the system assigns significance to the incident and then prioritizes it via color determination, from green (low priority) to black (an emergency).

In 2018, NEMA developed cyber hygiene and standards for electrical equipment and medical imaging device manufacturers to implement in order to help raise their level of cybersecurity sophistication in production facilities and engineering processes. These industry best practices are currently used by CMS member companies and are publicly available:

³ <https://www.congress.gov/bill/117th-congress/house-bill/2471/text>

⁴ [https://www.law.cornell.edu/definitions/uscode.php?width=840&height=800&iframe=true&def_id=6-USC-1080385210-](https://www.law.cornell.edu/definitions/uscode.php?width=840&height=800&iframe=true&def_id=6-USC-1080385210-773531972&term_occur=999&term_src=title:6:chapter:1:subchapter:XVIII:part:D:section:681)

[773531972&term_occur=999&term_src=title:6:chapter:1:subchapter:XVIII:part:D:section:681](https://www.law.cornell.edu/definitions/uscode.php?width=840&height=800&iframe=true&def_id=6-USC-1080385210-773531972&term_occur=999&term_src=title:6:chapter:1:subchapter:XVIII:part:D:section:681)

⁵ <https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>

⁶ <https://www.cisa.gov/uscert/CISA-National-Cyber-Incident-Scoring-System>

- **“Cyber Hygiene Best Practices: A NEMA White Paper.”** CPSP 2-2018:
<https://www.nema.org/standards/view/cyber-hygiene-best-practices>

Furthermore, NEMA has developed a set of complementary standards for end-users of such products. These best practices and guidelines are meant to help customers effectively manage their cybersecurity expectations as they use the equipment within the context of their respective markets, such as commercial buildings, the electrical grid, hospitals, and other PPD 21 critical infrastructure sectors. These standards can be publicly reviewed here:

- **“Cyber Hygiene Best Practices 2: A NEMA White Paper.”** CPSP 3-2019:
<https://www.nema.org/standards/view/cyber-hygiene-best-practices-part-2>

If not already incorporated, **NEMA strongly encourages CISA to adopt CPSP 2-2018 to the NCISS assessment lexicon.** In the event that a CMS electromanufacturer is required to report a cyber incident, NEMA insists that this standard be used in the assessment so that it can be triaged accordingly. Furthermore, **NEMA also advocates for the adoption of CPSP 2-2019 so that covered entities who have integrated electroindustry technologies into their systems can be appropriately assessed.** By applying these standards, the NCISS can help weed out or downgrade cyber events which may appear to be significant but in practice are not a high threat priority to critical infrastructure generally or to a company/industry.

(2) Report Contents and Submission Procedures

b. What constitutes “reasonable belief” that a covered cyber incident has occurred, which would initiate the time for the 72-hour deadline for reporting covered cyber incidents under section 2242(a)(1).

Electrical manufacturers rely heavily on operational technology (OT) systems in their production processes. OT refers to the hardware and software designated to detect or cause changes in the physical state of a system; in other words, they are the technologies which actually affect the real-world surroundings of an environment. If affected by a cyber incident, these technologies could disrupt or even modify information traffic and device functionality. This could result in physical harm to individuals, other systems, or have additional drastic consequences.

OT networks, generally, are not directly accessible to the internet due to their functional importance. They are segregated from information technology (IT) networks through air gaps, VPN devices, and routers/firewalls in order to prevent direct manipulation or compromise. A secure OT network is custom designed to achieve certain outcomes, given an owner’s/operator’s needs and resources. Due to the unique nature of each OT system, a threat actor seeking to attack such a system would need to have a high-level of education and understanding of system operations.

In establishing a timeline definition to constitute “reasonable belief” to begin the 72-hour reporting clock, CISA should give deference to the cybersecurity professionals tasked with defending OT systems belonging to a CMS entity. That individual will likely know or be able to know quickly the severity of an attack. Additionally, such a standard should be as objective as possible in order to prevent unnecessary and counterproductive administrative burdens on CMS entities. **The 72-hour clock on reporting to CISA the details of a cyber incident should begin once an unauthorized breach has been confirmed by a cybersecurity professional familiar with the targeted OT system.**

(3) Other Incident Reporting Requirements and Security Vulnerability Information Sharing.

a. Other existing or proposed federal or state regulations, directives, or similar policies that require reporting of cyber incidents or ransom payments, and any areas of actual, likely, or potential overlap, duplication, or conflict between those regulations, directives, or policies and CIRCIA's reporting requirements.

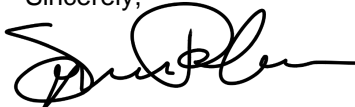
NEMA also represents manufacturers of medical imaging devices and equipment. Companies participating in the healthcare sector are generally regulated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which includes cyber security rules promulgated by the Department of Health and Human Services (HHS). As a result, many of these specific manufacturers develop products with cybersecurity in mind, since their ability to access the American healthcare market is determined on being able to meet HHS standards.

HIPAA-regulated entities are currently subject to cyber incident reporting requirements, including those found in both the HIPAA *Privacy Rule* and *Security Rule*.⁷ Taken together, these rules establish a national security standard for protecting certain health information that is held or transferred in electronic form. Over time, these rules have proven effective in creating an industry culture of security, a goal which CIRCIA seeks to replicate among non-regulated critical industry sectors.

To that end, CIRCIA authorized the creation of the Cyber Incident Reporting Council (Council) to review existing regulatory requirements and help ensure new reporting mandates avoid conflicting with or duplicating existing rules. Harmonization of reporting requirements is a critical component of this new law; bureaucratic roadblocks and unnecessary administrative burdens will greatly reduce the law's effectiveness and could even create aversion by covered entities to responsibly report covered cyber incidents in a comprehensive and timely manner. While CISA is not required by the law to incorporate the findings of the Council in its final rule, not doing would be counter to Congressional intent and would be impractical. Therefore, **NEMA strongly encourages CISA to consider and incorporate the findings of the Council to ensure incident reporting harmonization and efficiency throughout all industry sectors.**

NEMA once again appreciates the opportunity to submit comments on how the electroindustry can be a team player in developing guided and practical reporting requirements for critical manufacturing sector entities. If CISA has questions regarding these comments, please do not hesitate to contact me.

Sincerely,



Spencer Pederson
Vice President, Public Affairs

⁷ <https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html>