National Electrical Manufacturers Association

The Association of Electrical Equipment
and Medical Imaging Manufacturers
www.nema.org

May 9, 2022

Ms. Vanessa A. Countryman
Secretary
Securities and Exchange Commission
100 F Street NE
Washington, DC 20549-1090

RE: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (File Number S7-09-22)

Submitted via rule-comment@sec.gov

Dear Ms. Countryman:

The National Electrical Manufacturers Association (NEMA) welcomes the opportunity to provide comments to the Security and Exchange Commission's (Commission) proposed rule on *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*.

NEMA represents nearly 325 electrical equipment and medical imaging manufacturers that make safe, reliable, and efficient products and systems. Many of our member companies are considered part of critical infrastructure by the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), specifically within the critical manufacturing sector, meaning their operations are *"crucial to the economic prosperity and continuity of the United States*.[1]" Due to this important classification, NEMA has worked tirelessly for years encouraging all electroindustry companies, both publicly and privately owned, to make cybersecurity a key pillar of their organizational structure.

Electrical manufacturers believe that cybersecurity is a "team sport;" that the government and private sector share a dual responsibility to create a collaborative environment through the development of good policies and practices. Each part relies on the other for accurate, timely, and meaningful advice and support; a mutual trust that is built through practical and reasonable information sharing and disclosure between dedicated and responsible authorities, executives, and decision-makers. NEMA supports disclosure requirements that build upon and reinforce this principle of trust; however, the required dissemination of information to public audiences based upon a materiality standard, as the Commission proposes, is counterproductive. Such a standard does not include or expect any understanding of cybersecurity and would erode the bonds of this public-private partnership.

NEMA's comments will emphasize two aspects of cybersecurity which will also address many of the specific questions asked in the proposed rule: the need to understand **cybersecurity model distinctions** and the necessity of a **significant reporting standard**. As will be discussed below, most manufacturers rely on distinct and complex cybersecurity frameworks uniquely developed to safeguard operational technology (OT) and industrial control systems (ICS). Additionally, NEMA believes that because these cybersecurity models are distinct, cyber incidents should not be measured by a broad subjective standard. Further, only incidents that can be defined as significant, or having meaningful consequence which may cause real harm to operations and human safety, should be disclosed.

Cybersecurity Model Distinctions

Many electrical manufacturers operate highly sophisticated ICS which allow for production efficiency. ICS are generally comprised of integrated and proprietary OT to monitor and manage manufacturing equipment. OT differs from information technologies (IT) that generally comprise the information technology aspects of an organization that interact with consumers and human end-users. ICS include supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers. ICS allow manufacturers and other system operators to achieve high-level output goals which make them critical to American security and continuity, as well as a savory target for malicious cyber actors. An April 2022 joint cybersecurity advisory issued by the Department of Energy, CISA, the National Security Agency, and the Federal Bureau of Investigation (FBI) emphasize the constant and elevated risk ICS operators face[2].

Cybersecurity is not a tangible or specific thing; rather, it is a comprehensive strategy to secure systems based on their composition and intended function. (The Commission's proposed rule does not define cybersecurity.) IT systems and OT/ICS serve vastly different functions and, therefore, have different security requirements. Further, while a product may be produced to a certain manufacturing cybersecurity standard, how that product is applied and configured by an end-user could be held to a different standard. For example, NEMA has published its own set of cybersecurity best practices specific to electrical manufacturers and for the end-users of their products. These include:

- Cyber Hygiene Best Practices for Manufacturers (NEMA CPSP 2-2018)
  Industry best practices and guidelines to improve cybersecurity sophistication in manufacturing facilities and engineering processes.

- Cyber Hygiene Best Practices for End-Users (NEMA CPSP 3-2019)
  Industry best practices and guidelines for electrical and medical imaging manufacturers' customers to raise their level of cybersecurity sophistication as they utilize connected equipment.

The security standards that work for one entity, industry, or end user may not work for or apply to another. It is also necessary to consider that resources are finite; the strategies developed by companies to secure their systems are influenced by multiple variables such as funding/budget, access to knowledgeable human capital and expertise, and technical equipment availability.

Effective security strategies need to be aligned with postures which have been developed to protect their intended function. These postures cannot be subjective; they must be constructed using internationally recognized and understood frameworks that appropriately capture the scope of IT and OT/ICS applications. They also must be verifiable; OT/ICS conformity assessments are necessary for a system to protect against known threats and vulnerabilities. Numerous universally recognized frameworks for these operational systems currently exist, including (but not limited to):

- NIST Cybersecurity Framework
- IEC 62443
- NIST 800-53
- NIST 800-82
- ISO 27000 Series

Cybersecurity is complex and is rooted in objectivity, as the OT/ICS frameworks listed above demonstrate. However, the proposed rule seeks to establish a materiality standard as the trigger for

mandatory cyber incident reporting. Per the Commission's definition, materiality means that "*there is a substantial likelihood that a reasonable shareholder would consider it important*.[3]"

While a reasonable shareholder might find that cybersecurity is important, it is impractical to assume that they would understand the intricacies related to a cyber incident, including the nuances and subtle differences between IT and OT/ICS frameworks or operations. Without understanding the details of a registrant's cybersecurity postures, investors may not be able to accurately comprehend the impacts of various cyber incidents. Use of a materiality standard to require registrants to disclose sophisticated information and details about every cyber incident could risk oversimplifying the incident itself by trivializing the information reported to the Commission.

Information which is incomplete and without context or background does not help an investor make the best decision. NEMA reiterates that it supports disclosure requirements that build upon and reinforce trust, fosters mutual cooperation between industry and government, and furthers cybersecurity postures. As the proposed rule is currently written, we urge that the Commission not rush to implement a mandatory reporting criteria wholesale without first taking into account the potential security risks and negative financial impacts of publicizing information regarding an ongoing cyber incident.

Significant Reporting Standard

In March 2022, Congress passed the bipartisan Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA). The legislation identifies malicious actions that rise to a degree warranting attention by CISA as a 'significant cyber incident.' Per the legislative bill text, a 'significant' incident means:

> "*a cyber incident, or group of related cyber incidents, that the Secretary (of Homeland Security) determines is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the people of the United States*.[4]"

CISA's use of 'significant' as a triggering standard, rather than materiality, focuses on attacks that cause real harm. Further, CIRCIA authorizes the agency to determine what "covered cyber incidents" will need to be disclosed to the agency under that standard. Congress established a significant standard for cyber incident reporting to boost information sharing, partnership trust, and proper investigative analysis through an objective filter.

Materiality is overly subjective and is not a practical approach to increasing a company's cybersecurity posture. The proposed rule's use of a materiality standard breaks from Congressional intent and prioritizes investors' presumed interest above the cybersecurity of a registrant. During a cyber incident, this standard would force a company to focus on determining what information is deemed material to report rather than securing their systems. Proper disclosure should focus on first mitigating the cause of the incident, work with law enforcement authorities to investigate the incident, and then determine who is impacted. Following an objective-based process, rather than quickly pushing information out to the public, does put investor interest first by helping ensure their investment is secure and its value protected.

If the Commission is committed to improving cybersecurity postures, practices, and governance among registrants, we recommend that it not promote a policy standard that would have the opposite effect of making a company secure. NEMA strongly encourages the Commission to harmonize its triggering definition for disclosure with the CIRCIA standard of 'significant,' or develop an objective metric that can help registrants categorize what information is to be reported.

Cyber incident reporting based on an objective triggering threshold recognizes a key element: not all cyber incidents across economic sectors are momentous enough to warrant disclosure. For example, a cyber incident that is caused by employee error should not be viewed through the same focus as a company under assault from a malicious cyber group being funded by a hostile nation-state actor. The motivations behind a cyber incident also need to be fully understood; attacks against critical manufacturing registrants may occur to simply probe their cybersecurity posture, or to cause financial harm via ransomware extortion, or to cause physical harm by damaging OT/ICS.

Further, due to the strategic importance of registrants which are a part of critical infrastructure, it is expected that malicious cyber-attacks against them do and will continue to occur. However, not all of those incidents will rise to a level that warrant agency consideration or action, unless required by existing state or federal law. The distinction between cyber incidents prevents reporting authorities from being flooded with disclosures about incidents with little or no security value.

A deluge of cyber incident reports could undermine the proposed rule's intention of security through investor awareness by creating the false impression among shareholders that a registrant's cybersecurity posture is weak or ineffective. Continuous reporting using the same standard could create fatigue among investors, and the intended result of this proposed rule becomes further jaded. This could result in investors not responding appropriately to consequential cyber incidents because they have become indistinguishable from others.

NEMA firmly believes the public disclosure of a registrant's specific cybersecurity attestation models should not be made public. Revealing which frameworks and third parties constitute a registrant's security posture runs the high risk of violating contractual agreements and opens those third parties to liability risk and financial harm. It would allow competitors and malicious actors to ascertain details about a registrant's intellectual property through deduction, reverse engineering, and other methods. Unless investors have a direct role in the administrative functions and operations to a registrant's cybersecurity posture, there is no material value to be gained from having such information disclosed.

Additional Comments

Reporting Timeline & Confidentiality

The proposed rule states that a material cyber incident must be disclosed within four business days. NEMA supports disclosure timelines that allow for the most accurate intelligence regarding an incident to be gathered in order to present the best information to the required authorities. The Commission's proposed use of 'business days' to report an incident undermines the importance of cyber-threats and contradicts the intent of its proposed rule. The purpose of prompt incident reporting to CISA, the FBI, and other agencies is to address and remedy a cyber threat as soon as possible. To this end, these authorities have established specific reporting timeline language, i.e. the exact number of hours an entity has to submit a report.

According to the Department of the Treasury's definition, a 'business day' does not include Saturday, Sunday, a federal holiday, or any other day the SEC is obligated by law to be closed[5]. By using 'business day' as the reporting baseline, the sense of urgency is greatly diluted and gives the perception that cyber incidents are merely another element of business that can be handled during normal business/trading hours. If ensuring and bolstering a registrant's cybersecurity posture is an end-goal of this proposed rule, NEMA urges the Commission to reflect this motivation by adopting a specific reporting timeline. NEMA recommends that no reporting requirement should be less than 72 hours, so as to remain harmonious with other federal laws and reporting practices.

Additionally, and most importantly, any required disclosure should be protected and handled in a confidential and appropriate manner until an investigation has concluded. It is necessary to highlight that most cyber incidents are criminal in nature, intentionally carried out to disrupt and cause harm. As such, targeted registrants of cyberattacks are victims of crimes and should be offered due process. In practice, releasing information about a criminal action based solely on a materiality standard would punish the victim of an attack and could undermine an investigation. Publicly released information should be aggregated as much as possible to protect the reputation and market capitalization of a registrant.

NEMA recognizes and commends the Commission's attempt to see more registrants enhance their cybersecurity postures and make investors more aware of the importance of cybersecurity. However, for reasons stated above, the policy of public disclosure of sensitive cyber incident information through a materiality standard would undermine a registrants' cybersecurity. As mentioned in our opening, cybersecurity is a team sport and NEMA stands ready to be a willing partner on behalf of electroindustry registrants. We hope the Commission takes its time to develop refined reporting criteria that better enhances cybersecurity postures.

Sincerely,

Spencer Pederson
Vice President, Public Affairs

Endnotes

[1] https://www.cisa.gov/critical-manufacturing-sector

[2] https://www.cisa.gov/uscert/sites/default/files/publications/Joint_Cybersecurity_Advisory_APT%20Cyber%20Tools%20Targeting%20ICS%20SCADA%20Devices.pdf

[3] https://www.sec.gov/rules/proposed/2022/33-11038.pdf

[4] https://www.congress.gov/bill/117th-congress/house-bill/2471/text

[5] https://www.law.cornell.edu/cfr/text/31/802.201