National Electrical Manufacturers Association

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

November 3, 2023

National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Via email: cyberframework@nist.gov

RE: NEMA Comments on the NIST Cybersecurity Framework 2.0 Final Draft and its Related Implementation Examples Draft

The National Electrical Manufacturers Association ("NEMA") is submitting comments on the NIST Cybersecurity Framework 2.0 Final Draft and its Related Implementation Examples Draft. NEMA supports the overall direction being taken by the National Institute of Standards and Technology ("NIST") to update the *Cybersecurity Framework* ("CSF") to account for modern changes to the digital and cyber landscape since the publication of the CSF Version 1.1, including security risks, emerging technologies, and necessary resources.

NEMA is the leading trade association representing America's electroindustry: companies that manufacturer electrical and medical imaging equipment. Our more than 300 members produce safe, reliable, efficient, and secure products to serve seven key markets: building infrastructure; building systems; lighting systems; industrial products and systems; utility products and systems; transportation systems; and medical imaging and technology.

Electroindustry companies, particularly those deemed as critical infrastructure, take seriously their role in developing and strengthening the cybersecurity of their operational systems as well as the products they manufacturer. NEMA has created industry best practices, listed below, for electrical manufacturers to implement to minimize cybersecurity risk across supply chains and throughout operations. Furthermore, NEMA has created best practices for consumers to follow as they integrate manufacturers' products within their own systems so to help ensure products remain as secure as possible.

Below are those best-practice cybersecurity recommendations that NEMA will work to have incorporated into NIST's National Online Informative Reference Program.

1. **NEMA CPSP 1-2021**: *Supply Chain Best Practices* (https://www.nema.org/Standards/Pages/Supply-Chain-Best-Practices.aspx). This document identifies a recommended set of supply chain best practices and guidelines that electrical equipment and medical imaging manufacturers can implement during product development to minimize the possibility that bugs, malware, viruses, or other exploits can be used to negatively impact product operation.

2. **NEMA CPSP 2-2018**: *Cyber Hygiene Best Practices* (https://www.nema.org/Standards/Pages/Cyber-Hygiene-Best-Practices.aspx). This document identifies a set of industry best practices and guidelines for electrical equipment and medical imaging manufacturers to help raise their level of cybersecurity sophistication in their manufacturing facilities and engineering processes.

3. **NEMA CPSP 3-2019**: *Cyber Hygiene Best Practices-Part 2* (https://www.nema.org/Standards/Pages/Cyber-Hygiene-Best-Practices-Part-2.aspx). This document identifies industry best practices and guidelines that electrical equipment and medical imaging manufacturers may consider when providing cybersecurity information to their customers. These 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 (e.g., commercial, and residential buildings, industrial equipment, the electrical grid, hospitals, and surface transportation). The document also provides suggestions for how customers can work with their respective manufacturers to improve the customer's level of cybersecurity through industry best practices and guidelines.

NEMA provides the following general comments on the CSF 2.0 Final Draft:

1. NEMA supports the change of the title to the more commonly used name '*Cybersecurity Framework*' name and accompanying '*CSF*' acronym when referring to the framework. Such nomenclature allows NIST to appropriately scope the framework to broader audiences, thereby allowing its benefits to be more widely experienced by organizations and operations.

2. NEMA supports the relation of the CSF to other NIST frameworks and other relevant NIST publications.

3. NEMA supports the increased guidance on CSF implementation with action-oriented processes, framework profiles, and notional templates.

4. NEMA supports the inclusion of the crosscutting "Govern Function" as a core function in CSF 2.0 and strengthening its relationship to risk management and mitigation. NEMA has long supported the need for, and understood the importance of, a strong, well-defined, and clear governance role in cybersecurity and data risk management.

5. NEMA supports the direction to emphasize the importance of supply chain risk management ("C-SCRM") in the CSF 2.0, how it is integrated in the framework's Govern Function, and how well it is integrated across the other five functions. The integration of the Govern Function will allow organizations to establish appropriate supply chain risk

management regimes, with roles and responsibilities, and risk mitigation processes which are consistent with an organization's related capabilities. Its integration across the other five functions will provide a basis for supplier cybersecurity requirements that can be passed down to third party material suppliers and vendors. A supplier can then utilize existing techniques and best practices for managing and mitigating third party cybersecurity risks, including classifying supplier types/categories, vetting questionnaires; continuous risk monitoring through tools such as security ratings; and Service Level Agreements.

6. NEMA supports the direction of the CSF 2.0 to clarify the understanding and focus of cybersecurity measurement and assessment through tiers on cybersecurity governance, risk management, and third-party considerations.

NEMA provides the following general comments and recommendations on the Implementation Examples Draft:

1. NEMA supports the action-oriented implementation examples listed throughout each category and subcategory.

2. In subcategory GV.SC-05, there are several implementation examples that use the term contractually with respect to cybersecurity requirements of a supplier. NEMA agrees that, depending on the environment and risk assessment, a contract is an appropriate way to specify these types of requirements. It should also be noted that there are other methods suppliers utilize to address cybersecurity requirements, including the documentation of a product's examination or evaluation to a certain cybersecurity standard, and the documentation of a product stating utilization of a Secure Development Life Cycle which places security front and center during the product development.

The electroindustry will continue to be an active participant in this process. If you have any questions on these comments, please contact Steve Griffith, Executive Director, [redacted]

Respectfully,

Spencer Pederson
Senior Vice President, Public Affairs