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

National Electrical Manufacturers Association

April 25, 2022

Ms. Katherine MacFarland
National Institute of Standards and Technology
100 Bureau Drive (Mail Stop 2000)
Gaithersburg, MD 20899

Via email: CSF-SCRM-RFI@nist.gov

RE: NEMA Comments on the NIST Cybersecurity Framework- "NIST Cybersecurity RFI"

Dear Ms. MacFarland:

The National Electrical Manufacturers Association (NEMA) is submitting comments on the "NIST Cybersecurity RFI." NEMA represents more than 325 electrical equipment and medical imaging manufacturers that make safe, reliable, and efficient products and systems serving the following markets: buildings, lighting systems, industrial products and systems, utility products and systems, transportation systems, and medical imaging. We support 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, including security risks, emerging technologies, and necessary resources.

The electroindustry takes a serious role in developing and strengthening the cybersecurity of the products it manufacturers. NEMA has created and implemented industry best practices to minimize cybersecurity risk across supply chains, throughout operations, and within products themselves. The published best-practice documents referenced below include a series of viable recommendations for both equipment manufacturers and their customers. NEMA encourages NIST to refer to these documents when considering updates to the CSF, especially in regard to sections managing risk around operational technology (OT), industrial control systems (ICS), and legacy systems:

- **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.

- **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.

- **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.

With respect to the 14 topics provided by NIST identified in the request for information, NEMA provides the following comments:

USE OF THE NIST CYBERSECURITY FRAMEWORK

1. **The usefulness of the NIST Cybersecurity Framework for aiding organizations in organizing cybersecurity efforts via the five functions in the Framework and actively managing risks using those five functions.**

   NEMA believes that the five broad functions described in the CSF provide a common and usable lexicon of terminology for aiding entities of various sizes in organizing their cybersecurity efforts and actively managing their risks.

2. **Current benefits of using the NIST Cybersecurity Framework. Are communications improved within and between organizations and entities (e.g., supply chain partners, customers, or insurers)? Does the Framework allow for better assessment of risks, more effective management of risks, and/or increase the number of potential ways to manage risks? What might be relevant metrics for improvements to cybersecurity as a result of implementation of the Framework?**

   The CSF provides a good baseline for organizations seeking to identify, address, and manage cyber risk. The current framework is traceable to multiple internationally developed and recognized standards for those organizations and entities that would like to "step up" their cybersecurity efforts.

3. **Challenges that may prevent organizations from using the CSF or using it more easily or extensively (e.g., resource considerations, information sharing restrictions, organizational factors, workforce gaps, or complexity).**

   In its current version, the CSF is a very good baseline document, written in a general and high-level format. While NEMA recognizes the approach taken by NIST in using a generalized format, such a method presents a challenge for small organizations to improve their cybersecurity posture by not providing a recognizable or practical starting point. We suggest the CSF reference the Center for Internet Security (CIS) Controls (https://www.cisecurity.org/controls/cis-controls-list). These widely regarded security controls are a highly recommended set of actions that provide specific ways for organizations large and small to better defend against cybersecurity attacks by distilling key security concepts into actionable processes.

Additionally, NIST should seek to further engage with international standards organizations and equivalent government agencies on adoption and recognition of the CSF as part of their cybersecurity frameworks. Many NEMA members are a part of sophisticated manufacturing supply chains and whose OT/ICS products must conform to the cybersecurity standards required by the country in which they operate. Since the CSF is not a standard and applies primarily to an American/domestic business audience, other internationally accepted cybersecurity standards and practices are becoming de-facto security models. NEMA encourages NIST to use the CSF 2.0 as an opportunity to better harmonize the framework with foreign partners.

4. **Any features of the NIST Cybersecurity Framework that should be changed, added, or removed. These could include additions or modifications of: Functions, Categories, or Subcategories; Tiers; Profile Templates; references to standards, frameworks, models, and guidelines; guidance on how to use the CSF; or references to critical infrastructure versus the CSF's broader use.**

At a minimum, NEMA believes that both the *NIST Risk Management Framework* and the *NIST Privacy Framework* should be incorporated into any revision of the CSF. Additionally, NIST 800-82, which covers OT/ICS and includes and overlay of NIST 800-53 controls applicable to OT/ICS, should also be mapped into the CSF.

The revised CSF also needs to provide greater guidance on a variety of new and emerging technologies. This includes automation (and if manually controlled processes should or could incorporate automation). increased cloud security, tools and techniques related to penetration testing, best practices related to open-source software, and the inclusion of Common Vulnerabilities Enumeration (CVE).

5. **Impact to the usability and backward compatibility of the CSF if the structure of the framework such as Functions, Categories, Subcategories, etc. is modified or changed.**

NEMA believes that the usability of the framework is a key item for organizations that wish to implement it. We caution NIST against any overall structural change to the existing framework that might decrease its usability or substantially undermine security investment rooted in the original framework. Furthermore, we seek clarification and greater context from NIST around 'backward compatibility' and what the agency is specifically trying to achieve with a structural change to the CSF.

6. **Additional ways in which NIST could improve the CSF or make it more useful.**

   Other than what has already been stated, NEMA suggests that any changes made to the framework are identified to clearly distinguish between Version 1.1 and Version 2.0. NIST could also include a web-based mapping option.

RELATIONSHIP OF THE CSF TO OTHER RISK MANAGEMENT RESOURCES

7. **Suggestions for improving alignment or integration of the CSF with other NIST risk management resources. As part of the response, please indicate benefits and challenges of using these resources alone or in conjunction with the CSF. These resources include:**

   - **Risk management resources such as the NIST Risk Management Framework, the NIST Privacy Framework, and Integrating Cybersecurity and Enterprise Risk Management (NISTIR 8286).**

   - **Trustworthy technology resources such as the NIST Secure Software Development Framework, the NIST Internet of Things (IoT) Cybersecurity Capabilities Baseline, and the Guide to Industrial Control System Cybersecurity.**

   - **Workforce management resources such as the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity.**

   NEMA supports the effort to map these relevant frameworks into the CSF. Specifically, we encourage NIST to incorporate the appropriate role of governance functions and responsibilities into the CSF. NIST has identified the importance of governance functionality in mapping AI and data privacy risk; the interconnectedness between cybersecurity, data privacy, AI, and other emerging technologies requires that governance functions be addressed wholistically.

8. **Use of non-NIST frameworks or approaches in conjunction with the CSF. Are there commonalities or conflicts between the CSF and other voluntary, consensus resources? Are there commonalities or conflicts between the CSF and cybersecurity-related mandates or resources from government agencies? Are there ways to improve alignment or integration of the CSF with other frameworks, such as international approaches like the ISO/IEC 27000-series, including ISO/IEC TS 27110?**

   As noted in the answer to part 3 above, NEMA believes NIST should explore alignment and harmonization of the CSF with current recognized international cybersecurity standards, including the ISO/IEC 27001 series and the IEC 62443 series. It’s evident that NIST is already heavily vested and involved in international standards activities and advancing US interests; however, NEMA feels that these international standards organizations do not communicate sufficiently back to NIST. Most of the dialogue is one-way when it should be a mutual flow of communication and information.

9. **There are numerous examples of international adaptations of the CSF by other countries. The continued use of international standards for cybersecurity, with a focus on interoperability, security, usability, and resilience can promote innovation and competitiveness while enabling organizations to more easily and effectively integrate new technologies and services. Given this importance, what steps should NIST consider ensuring any update increases international use of the CSF?**

   NIST should expand the number of CSF foreign language translations, particularly languages spoken in countries integral to critical infrastructure supply chains, including critical manufacturing.

10. **References that should be considered for inclusion within NIST's Online Informative References Program (OLIR). This program is an effort to define standardized relationships between NIST and industry resources and elements of documents, products, and services and various NIST documents such as the CSF, NIST Privacy Framework, Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53), NIST Secure Software Development Framework, and the NIST Internet of Things (IoT) Cybersecurity Capabilities Baseline.**

    At a minimum the OLIR should include the following: the IEC 62443 series of standards, the ISO/IEC 27000 series of standards, and the (3) NEMA best practice documents that were described previously in this document: CPSP-1, CPSP-2, and CPSP-3.

CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT

11. **National Initiative for Improving Cybersecurity in Supply Chains (NIICS). What are the greatest challenges related to the cybersecurity aspects of supply chain risk management that the NIICS could address? How can NIST build on its current work on supply chain security, including software security work stemming from EO 14028, to increase trust and assurance in technology products, devices, and services?**

    One of the biggest challenges that the CSF could address is managing 3rd party suppliers. There are several techniques and best practices for managing 3rd party suppliers such as: classifying supplier types/categories, vetting questionnaires, continuous risk monitoring via tools such as security ratings, and even Service Level Agreements (SLAs) that the CSF could address.

12. **Approaches, tools, standards, guidelines, or other resources necessary for managing cybersecurity-related risks in supply chains. NIST welcomes input on such resources in**

narrowly defined areas (*e.g.*, pieces of hardware or software assurance or assured services, or specific to only one or two sectors) that may be useful to utilize more broadly; potential low risk, high reward resources that could be facilitated across diverse disciplines, sectors, or stakeholders; as well as large-scale and extremely difficult areas.

NEMA has no additional comments.

13. **Are there gaps observed in existing cybersecurity supply chain risk management guidance and resources, including how they apply to information and communications technology, operational technology, IoT, and industrial IoT? In addition, do NIST software and supply chain guidance and resources appropriately address cybersecurity challenges associated with open-source software? Are there additional approaches, tools, standards, guidelines, or other resources that NIST should consider achieving greater assurance throughout the software supply chain, including for open-source software?**

The NERC CIP Standards, which are the mandatory security standards that apply to entities that own or manage facilities that are part of the US and Canadian electric power grid, warrants consideration. The NERC CIP 013 Standard focuses on Cyber Security-Supply Chain Risk Management.

The IEC 62443 Series of Standards provide a systematic and practical approach to cybersecurity for industrial control systems. The Standards also provide a flexible framework to address and mitigate security vulnerabilities in OT/ICS. Every stage and aspect of cybersecurity is covered, from risk assessment through operations.

14. **Integration of the CSF and Cybersecurity Supply Chain Risk Management Guidance [e.g., see here]. Whether and how cybersecurity supply chain risk management considerations might be further integrated into an updated CSF—or whether and how a new and separate framework focused on cybersecurity supply chain risk management might be valuable and more appropriately be developed by NIST.**

NEMA believes that cybersecurity supply chain risk management considerations should be integrated into the updated CSF. A new or separate framework could cause additional confusion among organizations seeking to implement it.

Additional Comments

NEMA Members understand that for cybersecurity to be effective, it needs to be incorporated into a product's development and across its overall lifecycle, starting at its inception. While the methods used to protect information and systems vary across different technology platforms and operational environments, the process used to determine what information or systems must be protected is similar across global Standards and conformity assessment programs. This process-driven product development philosophy underpins many global cybersecurity Standards because it is a consistent way for all parties involved to evaluate their cybersecurity risk. Each individual Standard defines a particular process to evaluate that cybersecurity risk, and the resulting analyses are generally comparable.

When required, NEMA members demonstrate compliance or certification to global cybersecurity Standards via several assessment programs. Given that a compliance or certification program is providing a consistent way to evaluate an organizations cybersecurity process it stands to reason that the resulting certification could serve additional purposes beyond its original intent.

NEMA supports an open and inclusive process in the same way NIST developed the original *Framework for Improving Critical Infrastructure Cybersecurity (CSF)*. NEMA looks forward to remaining an active participant in this process. If you have any questions on these comments, please have your staff contact Steve Griffith, Senior Industry Director, at 703-307-7847 or Steve.Griffith@Nema.org.

Respectfully,

Spencer Pederson
Vice President, Public Affairs