National Electrical Manufacturers Association

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

March 8, 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 Concept Paper: Potential Significant Updates to the Cybersecurity Framework

The National Electrical Manufacturers Association ("NEMA") is submitting comments on the NIST Cybersecurity Framework 2.0 Concept Paper: *Potential Significant Updates to the Cybersecurity Framework* ("Concept Paper"). 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. 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.

Electroindustry companies, particularly those deemed as critical infrastructure, take seriously their role in developing and strengthening the cybersecurity of both their operational systems as well as the products they manufacturer. NEMA has created industry best practices for electrical manufacturers to implement in order 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. NEMA encourages NIST to reference these published best practice documents as it seeks to update the CSF, especially as it seeks industry- and sector-specific examples of cybersecurity models which can be built upon the five foundational concepts of the framework.

- **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.

NEMA provides the following comments and suggestions with respect to proposed CSF changes outlined in the Concept Paper:

1. **CSF 2.0 will explicitly recognize the CSF's broad use to clarify its potential applications.**

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

2. **CSF 2.0 will remain a framework, providing context and connections to existing standards and resources.**

   NEMA supports NIST's intent to retain the CSF's current level of detail; to clearly relate the CSF to other frameworks; to leverage more fully the recently launched Cybersecurity and Privacy Reference Tool for greater standards interoperability; to use updatable, online informative references to provide more guidance for CSF implementation; and, most importantly, to remain technology and vendor neutral to prevent and discourage vender-lock.

   NEMA agrees that mapping the CSF 2.0 to both ISO and IEC cybersecurity standards is a beneficial activity, particularly ISO 27001 and IEC 62443—standards widely used by electro manufacturers worldwide to mitigate risk in operational technologies (OT) and ICS. The mapping in CSF version 1.1 is not a true one-to-one correlation; the drafting of CSF 2.0 provides an opportunity to improve upon this discrepancy.

3. CSF 2.0 (and companion resources) will include updated and expanded guidance on Framework implementation.

OT/ICS Guidance

NEMA supports efforts to update and expand implementation guidance for CSF. As referenced above, NEMA has developed industry-specific cybersecurity best practices to reduce vendor and customer risk. As policymakers in Congress, the Department of Homeland Security ("DHS"), and throughout government continue realize the importance of OT as a co-equal to IT, it is important that updated guidance be provided. Better and more detailed implementation guidance could help manufacturers develop models which incorporate the broader concepts of the CSF with the more industry-specific and relevant recommendations by NEMA, ISA, IEC, and other standards organizations.

Public-Private Partnership Guidance

One of the biggest advantages of the CSF is the ability of companies and entities of various sizes and with varying business and operational models to adapt the core functions appropriately, based on their end goals. However, when entities with different goals and resources are required or encouraged to overlap, including through legislative or regulatory requirements, this could create a cybersecurity delta and increase the risk profile of all those involved. This increased risk could become a deterrence to achieving greater policy or economic goals.

Private and public entities are incentivized in different ways (for-profit vs. non-profit) and, therefore, approach cybersecurity generally from different perspectives. Yet, better resourced does not necessarily mean greater flexibility. Many private companies are subject to cybersecurity rules, regulations, and laws, depending on their industry, scope of business, company size, or product output. For example, an electro manufacturer that is classified as a critical manufacturing entity by DHS might need to dedicate ample financial, professional, and strategic resources to comply with mandates related to supply chain security, incident reporting, data security, and other requirements in addition to securing and maintaining their existing OT and IT systems.

The lack of cyber resources is especially true for public entities, particularly those in rural, remote, or disadvantaged communities. These groups tend to have the highest likelihood of having neither the financial abilities to appropriately invest in proper cybersecurity tools or techniques, nor have the best incentives to attract and retain suitable cybersecurity professionals. However, as the economy becomes ever-more interconnected, especially as the clean-energy transition continues to move forward aggressively, these public entities with meager means will be required to engage with private industry-sector entities which have significant cybersecurity operations and mandates.

NEMA encourages NIST to develop CSF guidance in the area of **public-private partnerships** to help bridge the resource divide and appropriately identify and reduce the

risk gap between these groups. Such guidance could build trust between such parties and even encourage the integration of overlapping core functions.

4. CSF 2.0 will emphasize the importance of cybersecurity governance.

NEMA supports the inclusion of a crosscutting "Govern Function" as a core function in CSF 2.0, as well as 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 understood governance role in cybersecurity and data risk management.

However, NEMA believes that governance should not be opened-ended and must be scoped appropriately. Executive roles should be as centralized as possible so that leadership and decision-making responsibilities are understood to avoid conflict or delay among executive-level personnel themselves. Further, such roles should be central in identifying, analyzing, prioritizing, responding to, and monitoring risks. Further, NEMA agrees that a Govern Function helps integrate other NIST-developed frameworks, including the *Privacy Framework* and the draft *AI Risk Management Framework*.

5. CSF 2.0 will emphasize the importance of cybersecurity supply chain risk management.

NEMA supports the direction of NIST to emphasize the importance of cybersecurity supply chain risk management (C-SCRM) in the CSF 2.0, and believes such considerations need to be integrated throughout the framework's five core functions.

However, NEMA questions how C-SCRM would be governed within the CSF 2.0. One significant related challenge is the risk management of 3rd party material suppliers and vendors. There are several identified techniques and best practices for managing such party's cybersecurity risks, including: classifying supplier types/categories; vetting questionnaires; continuous risk monitoring through tools such as security ratings; and Service Level Agreements. The CSF should consider how tools and practices such as these can be integrated into the core functions. Further, NIST should provide guidance on how an entity should interpret the scope C-SCRM.

6. CSF 2.0 will advance understanding of cybersecurity measurement and assessment.

NEMA supports the direction of the CSF 2.0 to advance the understanding of cybersecurity measurement and assessment. There needs to be consistent tools for assessing and measuring various cybersecurity models against existing standards, benchmarks which can be applied to and utilized across organizations and industry sectors. NEMA believes effective cybersecurity needs to be wholistic by design; security and risk management should be incorporated into a product's development starting at inception and continuing throughout its operational lifecycle. While a cybersecurity model used to protect data and systems might vary when applied across different

technology platforms and operational environments, the process used to determine its validity is similar across global standards and conformity assessment programs.

Following a process-driven philosophy that utilizes measurement and evaluation metrics from many globally recognized cybersecurity standards provides a consistent way for all parties involved to evaluate their risk and will also serve a dual purpose of evaluating an organizations effective use of the CSF.

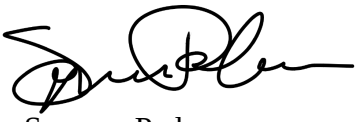
Each standard defines a particular process to evaluate a given cybersecurity risk, and the resulting analyses are generally comparable. For example, the EN 303 645[1] includes requirements for the manufacturer to have a unique password for all connected devices, establish a vulnerability management process, and publish a timeframe for providing security updates. This is similar to the unique password requirement for connected devices in the California IoT law.[2]

Electroindustry members demonstrate compliance or certification to global cybersecurity standards through several assessment programs. Given that these programs provide a consistent way to evaluate an organization's cybersecurity process, it stands to reason that the resulting certification could serve additional purposes beyond its original intent.

Additional Comments

NEMA supports an open and inclusive process in the development of CSF 2.0, in the same way NIST has done in its current and original version. 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, at [redacted]

Respectfully,



Spencer Pederson
Senior Vice President, Public Affairs

[1] https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf
[2] https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327