National Electrical Manufacturers Association

The association of electrical equipment
and medical imaging manufacturers
www.nema.org

November 8, 2021

California Privacy Protection Agency
Attn: Debra Castanon
915 Capitol Mall, Suite 350A
Sacramento, CA 95814

RE: Response to Invitation for Preliminary Comments on Proposed Rulemaking (Proceeding No. 01-21)

The National Electrical Manufacturers Association ("NEMA") is the leading trade association representing manufacturers of electrical and medical imaging equipment. The purpose of this letter is to introduce the electroindustry to the California Privacy Protection Agency ("Agency") as it invites public input and preliminary comments on proposed rulemaking under the California Privacy Rights Act ("CPRA") of 2020.

NEMA represents approximately 325 companies that manufacture safe, reliable, and efficient products and systems across 54 product sectors. Our combined industries account for more than 370,000 American jobs in more than 6,100 facilities covering every state. Additionally, the electroindustry produces $130 billion in electrical and medical imaging shipments annually, with $38 billion exported. In California specifically, 72 of our Member companies maintain 164 facilities, employing more than 24,000 people.

The products and systems NEMA Members produce are used and experienced by consumers daily in myriad ways, from smart lightbulbs in the home, to automated temperature control systems in connected buildings, to charging stations for clean electric vehicles. Many of these products are more effective in their application by the input of data received from consumers and their operating environments. Therefore, NEMA takes seriously the proper handling and processing of data and the security of that data from tangible and cyber threats.

The rich diversity of electroindustry products requires that NEMA Members invest significantly in developing and maintaining the integrity of supply chains rooted in privacy, security, and quality in order to bolster both public and private confidence in those products. Many products require the cybersecurity of operational technology ("OT") *in addition to* information technology ("IT"). This means that the Agency should not attempt to implement a single, "one-size-fits-all" approach to securing consumer data and control systems.

In making OT products secure, NEMA Members have collaborated with national and international Standards development organizations to create trusted and certifiable cybersecurity Standards, including:

- **National Institute of Standards and Technology ("NIST") Cybersecurity Framework** (https://www.nist.gov/cyberframework). The Framework is a widely used and respected set of guidelines and best practices businesses use to mitigate cybersecurity risks. The Framework allows a company to tailor and scale their cybersecurity posture based on their needs and resources. The Framework also incorporates elements from other cybersecurity Standards, including the two immediately listed below.

- **International Society of Automation ("ISA")/International Electrotechnical Commission ("IEC") 62443 Series of Standards** (https://www.isa.org/isa99/). These standards and technical reports relate to securing Industrial Automation and Control Systems ("IACS") by providing a

systemic and practical approach to cybersecurity for industrial control systems. They also provide a flexible framework to address and mitigate security vulnerabilities in IACSs. Every stage and aspect of cybersecurity is covered, from risk assessment through operations.

- **International Organization for Standardization ("ISO")/IEC 27001 Family of Standards** (https://www.iso.org/isoiec-27001-information-security.html). Also known as the ISO 27000 series, these Standards are a collection of best practices to help businesses improve their information security by specifying requirements in their information security management systems.

Additionally, NEMA itself has published the Cyber Secure Supply Chain ("CPSP") Series of Standards, viable best practice documents which many electrical and medical imaging manufacturers implement to secure in their supply chains, operations, and products from cyber threats. They include:

- **NEMA CPSP 1-2015**: **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.

The adoption of industry-developed, internationally recognized, and technology neutral cybersecurity Standards for IT and OT systems will be a critical component to ensuring the proper handling and processing of sensitive personal information by the electroindustry. The Agency should review these Standards, along with others, and incorporate them as appropriate into future proposal developments.

In its invitation, the Agency asks for input on the following topics:

> *What businesses that perform annual cybersecurity audits should be required to do, including what they should cover in their audits and what processes are needed to ensure that audits are "thorough and independent."*

Meaningful audits are rested in conformity assessments, where standardized requirements can be weighed against objective evidence and attested to by an independent party. As noted above, cybersecurity postures vary by technology application; therefore, cybersecurity audits should be performed using recognized Standards designed to validate a given posture. Electroindustry businesses

should be permitted to apply existing Standards and certifications, including conformity with the **NIST Cybersecurity Framework**, **ISA/IEC 62443**, **ISO/IEC 27001**, and the **NEMA CPSP** in meeting any Agency audit requirements.

> *When a business's processing of personal information presents a "significant risk to consumers' privacy or security".*

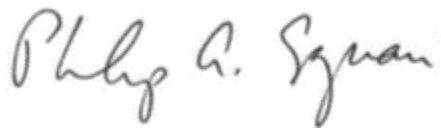
The Agency should define what a "significant risk" entails which might initiate a cybersecurity audit. Furthermore, the definition should be tailored to conform with the cybersecurity posture a business would be audited against.

> *What businesses that submit risk assessments to the Agency should be required to do, including what they should cover in their risk assessments, how often they should submit risk assessments, and how they should weigh the risks and benefits of processing consumers' personal information and sensitive personal information.*

After a company has submitted a risk assessment, additional assessments should not be required unless there has been a change in the Standards a company uses to be secure. This ensures that the Agency has the most current and accurate information for an evaluation. Furthermore, any risk assessment should align with the definition of "significant risk" referenced above.

NEMA counts on the Agency's careful consideration of these comments on behalf of the electroindustry. Agency decision-making will benefit from continuing its outreach to the regulated community, and NEMA plans to particulate fully in future proceedings on this important topic. If you have any questions or need more information, please contact Peter Ferrell, Manager, Connectivity and Data Policy, at 202-841-3200 or peter.ferrell@nema.org.

Sincerely,



Philip A. Squair
Vice President, Government Relations