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

National Electrical Manufacturers Association

October 6, 2023

Federal Communications Commission
Attn: Erika Olsen, Acting Chief, Cybersecurity and Communications Reliability Division
45 L Street NE
Washington, D.C. 20554

Submitted via website*: https://www.apps.fcc.gov/ecfs/*

RE: NEMA Comments on the Federal Communications Commission's ("FCC") Notice of Proposed Rulemaking ("NPRM") in the Matter of Cybersecurity Labeling for the Internet of Things: PS Docket No. 23-239

Dear Ms. Olsen:

The National Electrical Manufacturers Association ("NEMA") welcomes the opportunity to submit comments on the FCC NPRM in the matter of *Cybersecurity Labeling for the Internet of Things ("IoT").*[1] This rulemaking stems from the Administration's announcement of the "U.S. Cyber Trust Mark" program, launched to improve consumer confidence and understanding with respect to cybersecurity across IoT devices.

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. The Medical Imaging and Technology Alliance, which is an affiliated organization within NEMA, will be submitting separate comments to this NPRM, providing perspective specifically on medical imaging and technology.

Electroindustry companies, particularly those entities that produce consumer products, easily obtained or readily available (off-the-shelf) to the public, have long taken seriously their role in developing and strengthening the cybersecurity of both their operational systems and production processes, as well as the end-products they manufacturer. To bolster this claim, NEMA has created industry best practices for electrical manufacturers to implement in order to minimize cybersecurity risk across supply chains[2] and throughout

[1] https://www.federalregister.gov/documents/2023/08/25/2023-18357/cybersecurity-labeling-for-internet-of-things
[2] https://www.nema.org/standards/view/supply-chain-best-practices

operations.[3] Additionally, our organization has created complementary guidelines for consumers as they integrate manufacturers' products within their own systems to ensure security through implementation.[4] Furthermore, many electro-manufacturers routinely, and on a voluntarily basis, adopt and integrate industry consensus process standards and guidelines from both national and international organizations, including but not limited to the National Institute of Standards and Technology ("NIST"), the International Electrotechnical Commission ("IEC"), the International Society of Automation ("ISA"), the International Organization for Standardization, and the IoXT Alliance.

NEMA recognizes that governments worldwide are considering labeling as a means to effectively communicate cybersecurity features in consumer IoT products. While simple in concept, development and implementation of an effective labeling scheme is not as straight forward or easy. Cybersecurity postures vary depending on the type of product produced and its intended market audience and use, thereby complicating the creation of a comprehensive or one-size-fits-all solution in relaying the security level of a product. Additionally, while the intent of a label is to outwardly display that an item has been designed with some minimum level of cybersecurity in mind, it should not inadvertently create design disincentives. A new label should not undermine existing and internationally recognized cybersecurity standards which companies may have already integrated into their information technology and operational technology ("OT") systems and products.

For clarity, this NPRM is on the development of a label for IoT devices related to consumer products. OT is comprised of hardware and software that detects or causes a physical change through the direct monitoring and/or control of industrial equipment. OT devices are those that are not broadly defined as 'consumer' due to their usage in commercial operations and are not available or readily available for sale to the public. There exist numerous standards and conformity assessment schemes related to industrial OT systems, such as the ISA/IEC 62443 series of standards and conformity assessment programs, that provide a systematic, practical, and holistic approach to addressing cybersecurity. (The comments below focus on label development related to consumer IoT devices, not industrial IoT devices.)

NEMA provides the following specific comments, questions, and suggestions with respect to the discussion topics in the NPRM.

C. Establishing a Voluntary Cybersecurity Labeling Program.

7. NEMA supports the direction of the FCC to make this program voluntary. We agree with the comment that it will be dependent upon a willing and close partnership between the federal government, industry, and other stakeholders, key among them consumers.

[3] https://www.nema.org/standards/view/cyber-hygiene-best-practices

[4] https://www.nema.org/standards/view/cyber-hygiene-best-practices-part-2

A comprehensive and well-resourced education campaign will be critical so consumers can elevate their understanding of cybersecurity generally and what security features a label is attempting to relay. Additionally, such a campaign needs to highlight and warn consumers of the potential impacts and risks associated with unsecure or improper use of IoT devices in the event of a cybersecurity breach (i.e., physical life safety impacts, data privacy impacts, etc.). While this NPRM is based on the NIST 8425 Profile of the IoT Core Baseline for Consumer IoT Products, there are non-technical aspects and capabilities which need to be accounted for when the device is installed in a particular environment. A risk assessment can provide additional context for this.

D. Eligible Devices or Products.

10. This question asks if the NPRM should focus initially on IoT "devices" as defined in the document, specifically those wireless devices that intentionally emit radio frequency ("RF") energy." However, later in the same paragraph, it refers to the NIST IR 8425 definition of IoT devices as those devices "that have at least one transducer (sensor or actuator) for interacting directly with the physical world and at least one network interface (e.g., Ethernet, Wi-Fi, Bluetooth), for interfacing with the digital world."[5] This question also mentions if the FCC should include 'internet-connected' to the definition. By adding this, the program would encompass wireless gateways and interface modules that do not seem to fit within the scope of this program. **NEMA recommends the use of the NIST 8425 definition for the first version of the program.** This will avoid confusion to the consumer and make it clear that requirement applies to wired and wireless devices.

11. This question mentions that the program scope will focus on intentional radiators that generate and emit RF energy by radiation or induction. It also mentions that these devices, if exploited by a vulnerability, could be manipulated to generate, and emit RF energy that may cause harmful interference. While NEMA agrees that any IoT device may emit RF energy either intentionally, incidentally, or unintentionally, any such energy emitted due to exploitation may not be enough to cause harmful interference. **NEMA seeks clarification from the FCC on how harmful interference, or the absence of it, would be interpreted and documented within the scope of this program.** Also, since traditional FCC methods include emissions scans in all modes to detect harmful interference, is it the FCC's intent that something similar be done in this program? That process could be overly burdensome and time consuming for the consumer, assuming the consumer is educated to a degree to understand the complexity of this issue to make an appropriate purchasing decision.

[5] https://csrc.nist.gov/glossary/term/iot_device

12. This question asks if the FCC should focus the cybersecurity labeling program onto IoT "products" rather than IoT devices. **As stated above, NEMA prefers the rule adopt the NIST definition of 'IoT device,' and, therefore, we recommend that this labeling program focus only on IoT devices.** Further, and as a practical matter, smaller components that would constitute what the NPRM currently defines as a 'product' may not have enough physical space to accommodate a label. Labels do not need to expand beyond the device to additional components, such as backend systems, gateways, software, and mobile apps. It would be problematic for a backend system to be labeled, and, arguably, consumers do not need visibility into those aspects of a product.

    Labeling also becomes more complicated for manufacturers that ship products into multiple markets. Marking and labeling requirements can change after a product is shipped, and some manufacturers work with multiple certification providers. NEMA currently is working to ease the burden and complexity of physical product markings and labels through the promotion of e-labeling[6].

    It is noted that the NPRM is based on the NIST IR 8425 Profile of the IoT Core Baseline for Consumer IoT Products. In that document the technical requirements are referring to the 'IoT device' within the secure development process involving the product security context and its interaction with additional components (e.g.: backend, gateway, mobile app, etc.). To summarize, NIST is calling for the evaluation of the technical capabilities of the device in the context of the non-technical (process oriented) requirement of the product. NEMA agrees with the NIST summary and feels that the success of this program will be based on the ability to clearly articulate to consumers the benefits of participating devices.

13. As stated in our response to question 12, NEMA feels that the success of the program is to clearly articulate to consumers the benefits of labeled devices.

14. As stated in our response to question 12, NEMA feels that the success of the program is to clearly articulate to consumers the benefits of labeled devices. Consumer education is key for this program's success and there is no easy demarcation point if other components that make the IoT device functional need to be accounted for.

15. NEMA recognizes that IoT devices are prevalent in non-consumer settings like commercial, institutional, industrial, enterprise, or medical settings. Products in medical settings already have security obligations that are being enforced and regulated by the Food and Drug Administration ("FDA"). The FDA heavily regulates all aspects of medical

[6] https://www.nema.org/standards/view/NEMA-Position-Paper-on-Electronic-Labeling

devices, from product development through post-market management to product labeling. As noted in our opening statement above, **NEMA advises against broadly focusing this IoT labeling program onto non-consumer/commercial markets** and should apply this program narrowly and exclusively to consumer products.

E. Oversight and Management of the Proposed IoT Cybersecurity Labeling Program.

22. NEMA agrees that one entity should be responsible for overseeing and managing the labeling program. We have concerns that any third-party administrator may alter the overall scope and direction of the program thereby causing additional confusion in the market.

F. Development of IoT Cybersecurity Criteria and Standards

28. NEMA agrees with the direction to use NIST recommended IoT Criteria as the basis for the proposed labeling program and having it focus on cybersecurity outcomes rather than specific requirements. The mark should also recognize similarity in requirements from other standards such as IEC 62443-4-1 (secure development lifecycle) and IEC 62443-4-2 (technical capabilities) that demonstrate conformance to NIST 8425.

34. NEMA strongly recommends that a baseline conformity assessment program be developed through collaboration of all relevant stakeholders. There may be existing industrial conformity assessment schemes, such as the ISA/IEC 62443 Series of Standards, that could be used for an initial mapping process. Non-aligned cybersecurity conformity assessment programs increase complexity and confusion among IoT device manufacturers, which in turn increases costs and dramatically slows adoption of secure product in the market. As mentioned above, manufacturers worry that by not aligning a label with current assessment schemes, it creates an environment which actually disincentivizes the development of less secure products and undercuts the intent of the program altogether.

    NEMA agrees that the program should offer different methods for conformity assessment that are based on a risk assessment. A risk assessment will identify risks to the consumer by determining their probability of occurrence and their resulting impact. From this appropriate method for conformity assessment can be utilized such as: a manufacturer self-attestation that the product or device is complies to a certain cybersecurity standard, documentation that the product or device uses of a Secure Development Life Cycle that places security front and center during the product development, or third-party testing compliance via a Nationally Recognized Testing Laboratory.

35. NEMA recommends that the FCC consider a manufacturer's own self-assessment program as a viable means to determine compliance. It could work with manufacturers

to set clear guidelines for such a program, leveraging their existing processes and procedures to demonstrate cybersecurity compliance. As mentioned in our response to question 34, these include documentation that the device has been examined or evaluated to a certain cybersecurity standard or documentation stating utilization of a Secure Development Life Cycle that places security front and center during the product development.

G. Administering the IoT Labeling Program.

37. NEMA generally agrees with the use of a QR code or e-label to enable consumers to access more detailed information about the device or product.

42. NEMA agrees that Manufacturers provide End-of-Life ("EOL") and End-of-Service Life (EoSL) information on their devices and products to their customers. When the EOL period is reached manufacturers are no longer manufacturing the product or system. When the EoSL period is reached maintenance services, updates and patches are no longer available from the manufacturer. It's important that consumers are aware of this information so they can effectively plan for migrations, implementations, and disposal effectively. NEMA believes that this type of information is better stored electronically rather than on the label itself.

43. NEMA has concerns with the NRPM proposing the use of an 'IoT Registry' where the public may access a catalog of approved program devices. Namely we are skeptical as to who would administer and monitor this registry, where the resources to administer the registry would come from, how often and quickly such registry would be updated, and liability concerns stemming from the existence of a registry.

47. NEMA argues that manufacturers should not be liable or subject to fines or other duties on their IoT products or devices when they become aware of an unpatched vulnerability that poses security risks. Manufacturers have set plans to manage incidents and vulnerabilities that includes detection and recording, classification and initial support, investigation and diagnosis, resolution and recovery, closure, monitoring the progress of the resolution, and a communication plan to inform affected parties about the status of the resolution. Manufacturers also maintain communication channels with their customers as well as their upstream suppliers in order to keep abreast of any vulnerability issues and steps to mitigate the issues.

49. NEMA believes that the recommendation of an annual renewal period for the label would be extremely burdensome on manufacturers and difficult to practically maintain. Packaged devices that are labeled will often span multi-years in production and distribution before reaching the consumer. Manufacturers typically use market

surveillance programs to determine when to implement required cybersecurity updates and patches to their devices. The Commission should leverage these existing programs and work directly with the manufacturers to determine the appropriate period for label renewal.

54. The NOPR asks where a program participant has received authorization to utilize the label, does this represent an indicum of reasonableness that might serve as a defense or safe harbor against liability for damages resulting from a cyber incident? **In a word, "yes."**

    The label is intended to be an overt signal to a consumer that an IoT product is secure, to some level. It is also intended to persuade a consumer to purchase that product over a non-labeled one. Therefore, the power of the label will come from its ability to reward manufacturers who have invested in security; security which can and should be measurable and universally recognized. If a manufacturer builds a product which can be assessed and validated against current and independent standards, these additional design investments should be encouraged through some degree of a liability shield. A label with some level of legal guarantee will also be a step towards achieving the Administration's larger goal of overall market cybersecurity.

    In March of this year, the White House released its National Cybersecurity Strategy; the third pillar of the strategy seeks to "shape market forces to drive security and resilience."[7] Objective 3.2 within this pillar specifically refers to the need to drive and develop secure IoT devices. From the outset of the strategy, it acknowledges that Congress will need to authorize many incentives to encourage private sector participation in securing connected devices if it seeks to be successful in driving cheap, unsecure, and potentially dangerous products from the market. To help incentivize security-by-default/design and discourage first-to-market products, particularly consumer IoT devices, a labeling program should be attached to some form of liability protection or safe harbor.

    NEMA encourages the FCC to utilize any existing authorities it has which could provide liability protection to the labeling program. Additionally, as manufacturers of consumer IoT devices, the electroindustry welcomes the opportunity to work with the FCC to identify proper incentives which need to be authorized by Congress to further the FCCs mandate of this program and the strategy's overall goals.

Comment on Appendix A – IoT Product Criteria

NEMA has concerns with the language reflected in Appendix A. 7. F. i. which states:

[7] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

> *"... to ensure that IoT product and its product components are free of any known, exploitable, vulnerabilities."*

We request that the statement must be reworded as follows:

"…to ensure that IoT product and its product components are free of any known, exploitable vulnerabilities <u>based on risk assessment</u>."

The words "…based on risk assessment." are needed to avoid a scenario where every single known and exploitable vulnerability must be resolved. In many instances this might not even be practical or feasible, such as a low-risk exploitable vulnerability in a hardware component that has no adverse impact on the IoT product.

Additional Comments

NEMA also seeks clarification on how this NRPM would affect manufacturer compliance with existing FCC regulations. NEMA also requests that participating manufacturers receive safe harbor provisions for adopting the consumer labeling program.

NEMA supports an open and inclusive process in the development of this subsequent rulemaking like how NIST is developing the Cybersecurity Framework 2.0. 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 703-307-7847 or Steve.Griffith@Nema.org.

Respectfully,

Spencer Pederson
Senior Vice President, Public Affairs