



December 16, 2021

National Institute of Standards and Technology
Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Via email: labeling-eo@nist.gov

RE: NEMA Comments on the DRAFT Baseline Criteria for Consumer Software Cybersecurity Labeling

The National Electrical Manufacturers Association (“NEMA”) welcomes the opportunity to submit comments on the *DRAFT Baseline Criteria for Consumer Software Cybersecurity Labeling*. NEMA supports the overall direction taken by the National Institute of Standards and Technology (“NIST”) as a result of the *Presidential Executive Order 14028: Improving the Nation’s Cybersecurity* related to cybersecurity labeling for consumer software. However, we urge NIST to consider the following recommendations as it further develops its criteria.

NEMA is the leading trade association representing America’s electroindustry: companies that manufacture electrical and medical imaging equipment. Our approximately 325 Members produce safe, reliable, and efficient products serving six key markets: buildings, lighting systems, industrial products and systems, utility products and systems, transportation systems, and medical imaging. Of the products manufactured, they comprise goods intended for consumer consumption, including Internet of Things (“IoT”) and other connected devices.

NEMA recognizes that governments worldwide have considered labeling as a means to effectively communicate cybersecurity features in consumer products. Yet, as NIST is aware, software labeling is not a comprehensive or one-size-fits-all-solution given that cybersecurity postures vary depending on the type of product produced and their intended market audience. While labels may help incentivize adoption of cybersecurity in consumer software, they should neither be perceived as a substitute nor seek to undermine existing and internationally recognized cybersecurity standards which companies have already integrated into their information technology and operational technology systems and products.

Regardless of a product’s intended user-audience, NEMA has recognized the need for its Members to incorporate cybersecurity measures in their products for many years, starting at inception and continuing all the way through their products’ lifecycle. To this end, NEMA has published multiple electroindustry best-practice recommendations for both equipment manufacturers and their customers, including:

- **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.

In addition, NEMA recently published a whitepaper that emphasizes the need for globally harmonized cybersecurity process Standards and conformity assessment programs:

- **NEMA CPSP 4-2021** (<https://www.nema.org/standards/view/harmonized-cybersecurity-standards-and-conformity-assessment>). This document describes the key themes and rationale behind the need for a globally harmonized cybersecurity process that includes all aspects (both hardware and software) and how misalignment increases complexity and costs as well as slowing down market. The documents appendix lists out many of the Standards already being used by NEMA member companies across their corresponding markets.

NEMA recommends that NIST review and incorporate these industry-developed and recognized cybersecurity best-practices in its development of its labeling criteria.

With respect to the *DRAFT Baseline Criteria for Consumer Software Cybersecurity Labeling*, NEMA provides specific recommendations and comments:

- Section 1.2 Document Scope and Goals:

“...that software – that is, software normally used for personal, family, or household purposes...”

NEMA is pleased with NIST's definition of consumer software and requests that, at a minimum, this language be maintained in the final criteria document. However, further specification and exclusions will be needed to ensure that regulated products, including medical devices, are assessed in compliance to their specific regulation.

- Section 2.3.1.1 Software Provider

Attestation	<i>Software Provider</i>
Description	<i>Information relating to the entity that is making attestations in the label.</i>
Desired Outcome	<i>Consumers can quickly and easily determine the author/organization of the software that is making claims.</i>
Assertions	<i>The name of the software developer/vendor/owner making the claims in the label as well as the name and contact information for an individual within this entity that is responsible for these claims is readily available to the consumer.</i>

As written, the text within the “Assertions” description is too vague, specifically “the name and contact information of an individual.” Organizations change too rapidly for this to be a stable description. NEMA suggests that NIST require the name of a role or position within an organization be responsible for the claims. Furthermore, scenarios may exist where the software provider is more than one entity. Therefore, NEMA recommends the following text:

Assertions	<i>The names of all software developers/vendors/owners making the claims in the label as well as the role responsible for the claims within these respective entities is readily available to the consumer.</i>
-------------------	--

- Section 2.3.1.2 Label Scope

Attestation	<i>Label Scope</i>
Description	<i>A clear description of all software systems under the purview of the label that is readily understandable by the consumer. All other software required for the software to function but is outside the purview of the label should be described.</i>
Desired Outcome	<i>Consumers clearly understand what the attestations conferred by the label apply to. For example, if the attestations made in the label are only applicable to a mobile application running on a consumer’s mobile device, the Label Scope description should make this clear. This will enable consumers to better understand the security attestations made about the software as well as allow the consumer to better compare the characteristics of varying software products.</i>
Assertions	<i>The software provider attests to the completeness and correctness of the provided software description and this information is readily available to the consumer.</i>

As written, the “Description” is a blanket statement and needs more clarity and specificity on the level that needs to be described on the label. For example, would the level be similar to the National Telecommunications and Information Administration software bill of materials? Or, if the description is too specific, how will changes be reflected? Therefore, NEMA recommends the following text:

Description *A clear description of all software systems under the purview of the label that is in the expected level of understanding of the consumer.*

- Section 2.3.3.1 Free from Known Vulnerabilities

Attestation *Free from Known Vulnerabilities*

Description *The provider attests that known vulnerabilities have been fixed.*

Desired Outcome *Consumers should be confident when selecting software that it is free from known vulnerabilities.*

Assertions *The software provider asserts in good faith that as of the assertion date indicated in the label, the software is free from known vulnerabilities.*

As written, the requirements of this section are unachievable and unacceptable. It is unrealistic and impossible for a provider to attest to all known vulnerabilities, which in itself is a subjective expectation. Labels intended for consumer awareness must be limited to vulnerabilities that are known to be capable of exposing the consumer to harm. Furthermore, without a certifiable database of known vulnerabilities for verification at the time of production, enforcement of a labeling Standard is impossible.

While this document is not a Standard in and of itself, the final document could be adopted and enforced by labeling bodies, preventing organizations from adopting a voluntary labeling program. Therefore, due to the rationale provided above, **NEMA strongly recommends NIST remove this section from the final criteria document.**

- Section 2.3.3.3 Multifactor Authentication

Multifactor authentication is a highly effective cyber-hygiene practice, one that NEMA recommends in its best-practice document listed above: CPSP 2-2018. However, its application in non-commercial settings may complicate or prevent the functionality of operational technology and systems. This security feature's requirement depends on the type of functionality and data that requires protection. Since this baseline document is aimed at consumers, it should clarify multifactor authentication be encouraged as a best practice. Therefore, NEMA recommends the following text be added:

Assertions *The software provider makes one of the following assertions:*

Supports – *The software supports multifactor authentication or participates in an identity federation ecosystem that supports multifactor authentication.*

Non applicable – *The software provider does not require user authentication.*

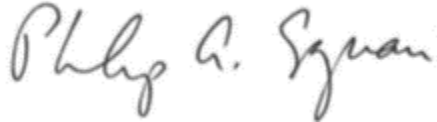
Applicable, non-supported – *The software provider does require user authentication but neither requires multifactor authentication nor participates in an identity federation ecosystem that supports multifactor authentication.*

Additionally, NEMA has general comments and suggestions regarding the DRAFT baseline:

- The document's focus is on consumer software. While some NEMA Members produce products for consumers, others do not. NIST should distinguish this further in and throughout the document.
- Within *Section 2.1: Methodology*, as written, the language does not express that a label by itself, particularly binary labels, may not be able to distinguish or compare software differences between dissimilar product types. For example, a software security label of a weather application may be totally different than that of a banking application. The average consumer will not know, or will not think to know, that the software used in each application is different just by viewing the label alone. The proposed level of detail in this section's attestations is only understandable to someone with a high-level understanding and education in software engineering.
- With regards to the "Label Scope" attestation within *Section 2.2: Terminology Conventions*, NEMA contends that it will be too complex and, therefore, difficult to be understood by the consumer. For example, the software running an application's user-interface may be secure, but the various back-end functions required to make the application work may be insecure. A consumer is not going to know or be able to discern between these differences. Furthermore, IoT devices exist in an ecosystem of products, software, and services that are mixed and managed by various software providers at various point in their design. It will be difficult for a label to express this in a way that makes sense to a consumer who has no background or education in software engineering.
- The document is intended to be guidance for consumer product software. The document is **not** a Standard; however, certification bodies could use it to build a voluntary labeling program providing advice and guidance on how NIST sees such a program being configured. NIST needs to keep this in mind as the document is further developed.
- NIST should align its efforts with testing, inspection, and conformity assessment organizations to ensure those entities develop certification criteria and have them report directly to the oversight group that NIST defines in this document.
- Many electrical products are small, and so too are their packaging. NIST should consider giving manufacturers multiple options for providing the information, including separate specification documents and QR codes to direct users to online resources.
- For attestation requirements presented in the document, NEMA recommends that NIST map out these requirements to the standards' frameworks and security controls, including existing frameworks established by NIST and the International Organization for Standardization and the International Electrotechnical Commission ("IEC"). Such a map could be in the form of an appendix. A map would help streamline requirements and promote their faster adoption.
- NEMA supports an open and inclusive process as this document is further developed, in the same way NIST developed the *Framework for Improving Critical Infrastructure Cybersecurity* ("CSF"). This document's concepts should align nationally with documents such as the CSF as well as internationally within such organizations as the IEC.

NEMA looks forward to remaining an active participant in this process. If you have any questions on these comments, please contact me or have your staff contact Peter Ferrell, Manager, Connectivity and Data Policy at Peter.Ferrell@Nema.org and Steve Griffith, Industry Director, at Steve.Griffith@Nema.org.

Sincerely,

A handwritten signature in black ink that reads "Philip A. Squair". The signature is written in a cursive style with a large initial "P".

Philip A. Squair
Vice President, Government Relations