Via labeling-eo@nist.gov

October 20, 2021

Katerina Megas
Program Manager, NIST Cybersecurity for IoT Program
National Institute of Standards and Technology
Gaithersburg, MD 20899

Barbara Cuthill
Deputy Program Manager, NIST Cybersecurity for IoT Program
National Institute of Standards and Technology
Gaithersburg, MD 20899

Subject: Draft *White Paper on Baseline Security Criteria for Consumer Internet of Things (IoT) Devices*

Dear Ms. Megas and Ms. Cuthill:

The U.S. Chamber of Commerce appreciates the National Institute of Standards and Technology's (NIST's) efforts in writing the draft *White Paper on Baseline Security Criteria for Consumer IoT Devices*.[1] We welcome NIST's outreach to the business community and the additional time to provide comments.

Key Points

- The Chamber values collaborating with NIST on an array of cybersecurity initiatives. The *Cybersecurity Framework* and the core security baseline for IoT devices represent two of the best examples of public-private partnerships in action.
- The administration, through NIST, is seeking feedback on government certification and/or labeling of IoT devices. Also, NIST is directed by the administration to examine ways to incentivize manufacturers and developers to participate in labeling programs.
- The Chamber welcomes NIST's considerable efforts on the white paper, but we strongly believe that the issue of IoT labeling must be handled through preemptive and protective federal legislation.

CHAMBER VALUES JOINT NIST-INDUSTRY PARTNERSHIPS

The Chamber values collaborating with NIST on an array of cybersecurity initiatives. The *Cybersecurity Framework* and the core security baseline for IoT devices represent two of the best examples of public-private partnerships in action.

The Biden administration, through NIST, is seeking feedback on government certification and/or labeling of IoT devices. Section 4 of the White House's Executive Order (EO) *Improving the Nation's Cybersecurity* calls on NIST to take into account existing consumer product labeling programs as it considers efforts to educate the public on the cybersecurity capabilities of IoT devices. Also, NIST is directed by the administration to examine ways to incentivize manufacturers and developers to participate in these programs. By early February 2022, NIST is required to identify IoT cybersecurity criteria for a consumer labeling program in coordination with the Federal Trade Commission and other agencies.[2]

The Chamber welcomes NIST's thoughtful diligence. However, the Chamber strongly believes that the issue of IoT labeling must be handled through preemptive and protective federal legislation. The Chamber expressed similar thinking in a letter sent on October 18, 2021, to the Federal Communications Commission.[3]

The Chamber recognizes that NIST cannot write and pass legislation. But simply commenting on the white paper criteria would miss the big picture, and the role of Congress needs to be a central part of the discussion on strengthening IoT cybersecurity. The Chamber contends that the labeling of IoT devices, absent an expressly preemptive and protective bill, would essentially be putting the policy cart before the legislative horse.

CONGRESS NEEDS TO PASS PREEMPTIVE, PROTECTIVE IOT CYBERSECURITY LEGISLATION

Fragmented approaches to IoT cybersecurity lead to duplicative and/or confusing security requirements, splinter organizations' risk management budgets, and cause market distortions that weaken security for individual companies and collectively. The Chamber believes that the path forward is relatively straightforward but not easy. Congress must pass a federal, preemptive law that both addresses IoT cybersecurity and extends legal liability protections to industry. Such a law would have the virtues of giving policymakers, the business community, and consumers more of what they need.

The administration is seeking ways to increase the presence of trusted equipment on U.S. networks and information systems and spur innovation in more securable devices. Industry seeks these outcomes too. In addition, businesses need policymakers to better balance federal regulation with legal liability and related protections, consider the growing private sector costs of defending against nation states, and harmonize and promote U.S. policies at home and internationally.

A useful way to think about this model legislation is to summarize it in three P's: program, protection, and preemption.

Program. The Chamber strives to work with lawmakers to strengthen the cybersecurity environment for governments, businesses, and consumers. We are especially interested in advancing innovative cybersecurity policies and laws that carefully balance regulatory compliance with industry-recognized standards and positive incentives to increase U.S. security and resilience commensurate with today's threat levels.

Congress should write federal IoT cybersecurity legislation to motivate businesses to demonstrate their use of existing standards, guidelines, and frameworks to meet a regulation's and/or a law's requirements. In exchange, businesses would qualify for congressionally crafted protections and other inducements to invest in and meet heightened cybersecurity requirements. Where applicable, legislation should offer private parties a range of appropriate standards, guidelines, and/or frameworks to select from, facilitating choice and the buy-in of parties that may be subject to various regulatory requirements or expectations.[4] Relatedly, programs should establish reciprocity requirements in order to harmonize laws, regulations, and other obligations. Congressionally created programs should be flexible—such as scalable to a business' size and budget, and risk based—thus targeting industry's resources at legitimate threats and harms.

Protection. Businesses confront relentless, often state-sponsored, cyberattacks but frequently lack effective government protection. Cyberspace remains the only domain where private companies are expected to defend themselves against nation states and/or their proxies. The Chamber believes that this security gap justifies blending a mix of new cybersecurity requirements with regulatory and legal protections.[5]

The Chamber believes that Congress should incentivize the behavior of industry members by granting robust legal liability protections. These safeguards would benefit organizations that take additional steps to elevate IoT cybersecurity. Depending on the nature of an IoT cybersecurity program, legal liability protections should range from an affirmative defense (sometimes referred to as a safe harbor) against lawsuits to more comprehensive protections against litigation generated by a cyberattack if a business is a builder, seller, or user of a government-driven certification and/or labeling program.

The Chamber is concerned about government-driven certification and/or labeling programs related to cybersecurity, including their costs, absent some offsetting incentive structure. There is no public-private consensus that IoT device labeling is a silver bullet, even if labels empower consumers and other device users to make decisions based on security.[6] NIST's pilot programs and related work on IoT labeling must be given the opportunity to develop with substantial industry input without predetermined outcomes.

Yet if policymakers are confident that government-directed certification and/or labeling regimes would deliver the cybersecurity that these programs tend to presume, then certifications/labels should be confidently paired with legal liability protections for producers, sellers, and users of stronger IoT devices. Authorizing legal liability protections for industry

would be the surest way to bolster the presence of trusted IoT equipment on U.S. networks and information systems.

Preemption. As new cybersecurity laws continue to be enacted domestically and internationally, businesses are forced to navigate a crowded patchwork of obligations. Adopting risk-based legislation while establishing clear and consistent federal guidelines would ensure that both regulators and regulated entities can direct scarce resources at significant cybersecurity risks. Congress should expressly preempt state IoT cybersecurity laws to provide national uniformity and align duplicative and often conflicting compliance burdens. Greater business certainty would drive investments in better cybersecurity risk management and adherence to laws and requirements.

***

The Chamber believes that stakeholders should increasingly direct their energies toward accomplishing two goals that will bolster the promotion of the baseline: fostering market demand for strong devices and pushing public officials at home and internationally to align their policies to the industry-driven IoT cybersecurity baseline.

***

COMMENTS ON THE WHITE PAPER

The remainder of this letter consists of feedback from the business community, which ranges from high level to specific, that the Chamber has received on the white paper. Some respondents disagree about elements of the white paper and their implications for IoT devices. The Chamber does not necessarily endorse each view, but we believe that NIST should consider each in the context of the cybersecurity stakeholders' comments.

Table 1: IoT Product Cybersecurity Capabilities Developed From NISTIR 8259A Using Informative References

A company told the Chamber that table 1 should be revised to reflect that antimalware/endpoint security is required for devices with operating systems (e.g., Debian Linux). For these and other less intelligent systems, memory/firmware scanning should be provided.

Page 4

- The Data Protection Capability should specify transport layer security (TLS) 1.3 for data in transit.

- The Logical Access to Interfaces capability should include multifactor authentication (MFA)/certificates for privileged access.

- The Software Update Capability should require signed software.

Page 5

- The Cybersecurity State Awareness capability should require logs sent to security information and event management (SIEM)/log collection.

- The Product Security capability would be better termed "resilience." The criteria note that a device should continue operating in the event of a network outage, but the time frame (e.g., hours or days) would likely depend on the product category.

Table 2: Non-Technical Supporting Capabilities Developed From NISTIR 8259B Using Informative References

Pages 5–7

- The white paper (p. 6, 5.a.) says, "All hardware and software components, from all sources (e.g., open source, propriety third-party, internally developed) used to create the IoT product" should be documented. The company told the Chamber that the white paper should be revised to simply reflect that a Software Bill of Materials (SBOM) is needed, as well as software component analysis for all open-source code.

- A business disagreed, telling the Chamber that SBOMs are "too complex for most consumers to understand well, and they do not add any utility for the consumer. Keep labeling easy to understand."

- One association told the Chamber that NIST noted in an October 14, 2021, workshop on the cybersecurity EO[7] that an SBOM is not yet demonstrably mature enough to be required, which is in keeping with the views of a substantial number of cybersecurity stakeholders. The association added that NIST should "proceed cautiously before making a blanket endorsement of an SBOM."[8]

- The company said documentation should include a report showing that the code has been scanned for vulnerabilities and what, if any, vulnerabilities exist, such as based on NIST's Common Vulnerabilities and Exposures (CVE) listing, which feeds the National Vulnerability Database (NVD) program.

- The business expressed caution, saying, "Any disclosure of vulnerabilities should focus on critical vulnerabilities and not overwhelm a consumer with a sea of information about false positive or low risk vulnerabilities."

- **Information Dissemination.** The company said criteria 2.b. (p. 7) mentions "vulnerability alerts" but should specifically call out NIST's Common Vulnerability Scoring System (CVSS), which is an open framework for communicating the characteristics and severity of software vulnerabilities, and NVD-CVE.

- **Threat Model.** The company said that "a requirement [of the manufacturer] to develop a threat model for expected use cases should be included in the non-technical supporting

capability criteria. This addition would align the criteria with other international standards and recommended best practices."

Table 3: Potential Additional IoT Product Criteria Developed From NISTIR 8259A Using Informative References

Page 9

- **Cybersecurity State Awareness.** The company told the Chamber that this capability should include "log collection and monitoring of systems."

Increasingly Comprehensive Levels of Testing and Assessment (Tiers)

The company told the Chamber that the "tiered approach mentioned but not detailed in the white paper [p. 10] should be maintained and elaborated upon so that it would align with established international regulatory programs and voluntary industry-led cybersecurity standards." The company added, "Security is not a binary proposition, but a gradient. Different products should have different security capabilities and purchasers would have varying preferences and expectations."

Conformity Assessment Approaches

NIST says that "existing labeling schemes utilize several approaches to demonstrate that consumer IoT devices conform to defined technical requirements, either exclusively or in combination." These schemes include a supplier's declaration of conformity (self-attestation), third-party testing or inspection, and third-party certification (p. 10).

The company told the Chamber that the conformity assessments of IoT devices should "leverage third-party examinations performed by accredited bodies according to existing international standards." A global but still immature IoT product market is developing. Even good-faith efforts to interpret criteria can vary widely, the company said. "Many small firms lack the expertise to evaluate whether their processes and capabilities would meet labeling requirements. Use of certified labs brings consistency and lessens the likelihood of bad faith actors," the company added.

In contrast, the business said, "No—conformity should be based on a self-assessment. Otherwise, it would be impossible to scale assessments, and they would only benefit the consulting companies that are hired as third-party assessors. The administration should focus on self-assessments, which can scale and provide meaningful labeling."

"Consumer" definition. The company remarked that the term "consumer" in the context of the white paper seems intended to include all potential users. However, this is not clear. The term

"consumer" carries context implications leaning toward home users and small businesses more than sophisticated large enterprises, government agencies, or industry. The company suggests that utilization of a term such as "purchaser" or "asset owner" would potentially have fewer connotations. An explicit statement of limitation should be considered regarding applicability, such as "these requirements may not be sufficient for industrial or enterprise use."

NISTIR 8259A requirements. The company said that some of the capabilities included in NISTIR 8259A but not in the white paper, especially software update, should be reconsidered for explicit inclusion in baseline security criteria. Moreover, "protective measures such as rollback prevention and automatic updates should be available and enabled by default but should also be configurable by the end-user," the company said. While such measures may be addressed by the requirements regarding product configuration, the white paper does not explicitly state what should be configurable. The company stresses that "these are important parameters for many use cases, and they are addressed explicitly in several standards, including ETSI in provision 5.3-6[9] and other international standards.

Product orientation. The company told the Chamber that the "purchaser is not obtaining an independent device that has its own freestanding utility. Even a device that retains some functionality without being connected is software dependent, with the full functionality that is marketed being dependent on nonlocal components." According to the company, "The IoT labeling program should address the entire product—device, software (e.g., a mobile app), communications, and cloud services." Further, "Hubs should be included when they provide required functions, and the full capability of the product cannot be delivered without it. It is especially important to address the software and services as the highest likelihood of compromise will be present at the cloud layer," the company said.

"No," the business stressed to the Chamber. The administration should "focus on IoT devices and applications that interact with the consumer. Do not overcomplicate IoT device labeling by expanding the scope to all software. This effort needs to focus on what the consumer cares about—that is, their device or application, not the components underlying the device or application."

Lifecycle emphasis. "Labels are static, but risks are not. Purchasers need to know up front what the expected life and terms of support would be, and they need to be equal. An explicit statement about the expected product life and support period can address the widely different lifecycles among devices (e.g., monitoring cameras and refrigerators). The white paper should be revised to communicate what the end-of-life process would mean to consumers and what actions they would likely need to take. It is well known that devices completely stop functioning at the end of support, even if there were functions of the product that did not require services.

***

The Chamber welcomes the opportunity to provide NIST with comments on the draft white paper. If you have any questions or need more information, please do not hesitate to contact Christopher Roberti (croberti@uschamber.com, 202-463-3100) or Matthew Eggers (meggers@uschamber.com, 202-463-5619).

Sincerely,

Christopher D. Roberti
Senior Vice President
Cyber, Intelligence, and
and Supply Chain Security

Matthew J. Eggers
Vice President
Cybersecurity Policy

Endnotes

---

[1] https://www.nist.gov/system/files/documents/2021/08/31/IoT%20White%20Paper%20-%20Final%202021-08-31.pdf
https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/iot-device-criteria

[2] The White House, Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*, March 12, 2021. https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

National Institute of Standards and Technology (NIST), "Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software."
https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/cybersecurity-labeling-consumers-internet-things

[3] https://www.fcc.gov/ecfs/filing/10182049018274

[4] The 2018 Ohio Data Protection Act (S.B. 220) is a notable model that the Chamber supports. Ohio enacted this innovative data security/cyber law in November 2018. S.B. 220 grants an affirmative defense against data breach tort claims to those businesses whose cybersecurity plans leverage an acceptable industry standard; other states' data protection laws focus on requirements or penalties. The Ohio statute uses an affirmative defense to incentivize companies to improve their cyber practices.
https://moritzlaw.osu.edu/data-and-governance/wp-content/uploads/sites/105/2019/03/cybersecurity-whitepaper-32819F-1.pdf

[5] The Cybersecurity Information Sharing Act of 2015 (see title N of P.L. 114-113), which had the support of both parties in Congress and the Obama administration, is a good example of a program that encourages businesses to defend their computer systems and share cyber threat data with government and private entities within a protective policy and legal structure.
https://www.congress.gov/bill/114th-congress/house-bill/2029

[6] For a range of perspectives on IoT device labeling, see NIST's "Workshop on Cybersecurity Labeling Programs for Consumers: Internet of Things (IoT) Devices and Software," September 14–15, 2021. https://www.nist.gov/news-events/events/2021/09/workshop-cybersecurity-labeling-programs-consumers-internet-things-iot

[7] NIST, "Improving the Nation's Cybersecurity: Progress and Next Steps in Carrying Out Executive Order 14028," October 14, 2021. https://www.nist.gov/news-events/events/2021/10/improving-nations-cybersecurity-progress-and-next-steps-carrying-out

[8] See the Chamber's comments to the National Telecommunications and Information Administration on Software Bill of Materials (SBOM) elements and considerations, June 17, 2021. https://www.ntia.doc.gov/files/ntia/publications/uscc_-_2021.06.17.pdf

[9] ETSI, *Cyber Security for Consumer Internet of Things: Baseline Requirements, ETSI TS 103 645 v2.1.2 (2020-06)*, p. 16. https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/02.01.02_60/ts_103645v020102p.pdf