U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

Via labeling-eo@nist.gov

December 16, 2021

Michael Ogata
Applied Cybersecurity Division
National Institute of Standards and Technology
Gaithersburg, MD 20899

Subject: Draft Consumer Software Labeling Criteria

Dear Mr. Ogata:

The U.S. Chamber of Commerce values the National Institute of Standards and Technology's (NIST's) efforts in writing the draft *Baseline Criteria for Consumer Software Cybersecurity Labeling*,[1] and we appreciate NIST's outreach to the business community on the white paper and related issues.

The Chamber also appreciates collaborating with NIST on an array of cybersecurity initiatives. The Cybersecurity Framework and the baseline security criteria for internet of things (IoT) devices[2] represent optimal examples of public-private partnerships in action.

In this latest white paper, the Biden administration, through NIST, is seeking feedback on the cybersecurity labeling of consumer software.[3] The Chamber recognizes NIST's considerable efforts on the draft document, but we do not comment on elements of proposed consumer software labeling criteria. We believe that the issue of labeling and possible certifications—whether for IoT devices/products[4] or consumer software—should be addressed through preemptive and protective federal legislation.

Key Points

- The administration, through NIST, is seeking feedback on cybersecurity labeling programs for IoT products and consumer software, including market incentives.
- The Chamber is concerned about labeling and/or certification programs related to cybersecurity, including their costs, absent some offsetting incentive structure. There is no public-private consensus that labeling is a silver bullet, even if labels empower consumers to make decisions based on security.
- If policymakers are confident that labeling programs would deliver the cybersecurity benefits that these efforts suggest, then labels should be paired with legal liability protections for the producers, the sellers, and the users of stronger IoT products and consumer software.

In October 2021, the Chamber advocated for a preemptive and protective approach to cybersecurity labeling in a letter to NIST regarding the agency's draft *White Paper on Baseline Security Criteria for Consumer Internet of Things (IoT) Devices*.[5] Also, the Chamber argued for similar thinking in a letter that we sent to the Federal Communications Commission on the agency's notice of inquiry pertaining to ways to strengthen IoT cybersecurity.[6]

The Chamber recognizes that NIST cannot write and pass legislation. Yet simply commenting on the draft baseline criteria for IoT products and/or consumer software labeling would likely overlook the big picture, including the role that Congress should play in discussions on cybersecurity.[7]

Safe Harbor Model Policy Is a Win-Win for Government and Industry Stakeholders

The working model that the Chamber envisions would provide a blueprint for policymakers to encourage businesses to invest in cybersecurity, which would ultimately increase U.S. security and resilience to reduce cybersecurity incidents. The model—featuring the combination of a *voluntary* labeling program and a legal safe harbor—acknowledges the need to encourage businesses to achieve a higher level of cybersecurity through voluntary, nonregulatory action, which is consistent with the aims of NIST and the administration.

Congress Should Pass Preemptive, Protective IoT Product and Consumer Software Cybersecurity Legislation

Fragmented policy approaches to IoT product and consumer software 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 should pass a federal, preemptive law that both addresses IoT product and consumer software 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.[8]

The administration is seeking ways to increase the presence of more securable products on U.S. networks and reduce vulnerabilities in software. Industry seeks these outcomes too. At the same time, 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 product and consumer software 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.[9]

Relatedly, programs should establish reciprocity requirements to better harmonize laws, regulations, and other obligations. Congressionally created programs should be flexible—scalable, for example, 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.

The Chamber also 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 product and consumer software cybersecurity. Depending on the nature of a labeling program, legal liability protections should range from 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 labeling and/or certification program.

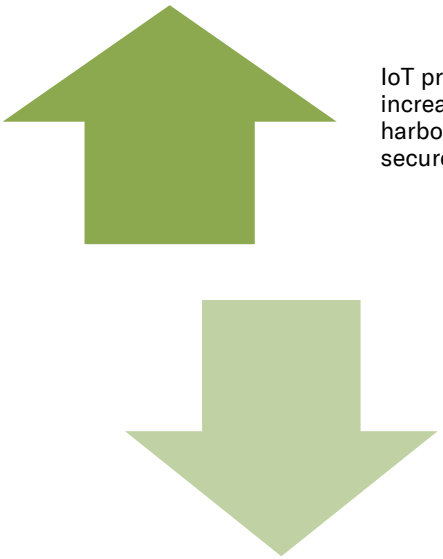
The Chamber is concerned about labeling and/or certification programs related to cybersecurity, including their costs, absent some offsetting incentive structure. There is no public-private consensus that labeling is a silver bullet, even if labels empower consumers to make decisions based on security.

If policymakers are confident that labeling and/or certification regimes would deliver the cybersecurity that these programs tend to suggest, then labels/certifications should be confidently paired with legal liability protections for the producers, sellers, and users of stronger IoT products and consumer software. Authorizing legal liability protections for industry would be the surest way to bolster the presence of trusted IoT equipment and consumer software 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 product and consumer software 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.

Increased Product and Software Security Would Reduce Market Uncertainty



IoT product and consumer software security would increase in connection with an established legal safe harbor, including an uptick in market demand for more secure and protected technology.

Market uncertainty would decrease as more and more IoT products and consumer software conform with programs that extend liability protections to both the makers and the buyers of labeled technology.

***

The Chamber appreciates 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, 202-536-7674).

Sincerely,

Senior Vice President
Cyber, Intelligence, and
and Supply Chain Security

Matthew J. Eggers
Vice President
Cybersecurity Policy

Endnotes

---

[1] https://csrc.nist.gov/publications/detail/white-paper/2021/11/01/baseline-criteria-for-consumer-software-cybersecurity-labeling/draft
https://www.nist.gov/system/files/documents/2021/11/01/Draft%20Consumer%20Software%20Labeling.pdf

[2] National Institute of Standards and Technology (NIST) draft *Baseline Security Criteria for Consumer IoT Devices*, August 31, 2021.
https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/iot-product-criteria
https://www.nist.gov/system/files/documents/2021/08/31/IoT%20White%20Paper%20-%20Final%202021-08-31.pdf

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

[4] NIST document *Consumer Cybersecurity Labeling for IoT Products: Discussion Draft on the Path Forward*, December 3, 2021. According to NIST, "In the context of this labeling scheme, an IoT product is defined as an IoT device and any additional product components that are necessary to using the IoT device beyond basic operational features" (p. 2).
https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/iot-product-criteria
https://www.nist.gov/system/files/documents/2021/12/03/FINAL_Consumer_IoT_Label_Discussion_Paper_20211202.pdf

[5] https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/iot-product-criteria
https://www.nist.gov/system/files/documents/2021/10/29/37-US%20Chamber%20Comments_DraftCriteria_IoTLabeling_NIST.pdf

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

[7] The Chamber's concerns about liability are not abstract. The Cyberspace Solarium Commission (CSC) pushed Congress to establish liability for final goods assemblers. See recommendation 4.2 in the CSC's March 2020 report. The CSC asserts that Congress should enact legislation establishing that "final goods assemblers of software, hardware, and firmware are liable for damages from incidents that exploit vulnerabilities that were known at the time of shipment or discovered and not fixed within a reasonable amount of time," among other recommendations.
https://www.solarium.gov

[8] In December 2020, the IoT Cybersecurity Improvement Act of 2020 (the IoT Act) became law after some three years of development. Among other things, the law establishes minimum security requirements for IoT devices purchased by the U.S. government. However, notwithstanding industry urgings, Congress stopped short of developing a national, protective bill that addressed the underlying costs of increasing domestic policy fragmentation, which the IoT Act contributes to.

The IoT Act (P.L. 116-207).
https://www.congress.gov/bill/116th-congress/house-bill/1668

Also see the Chamber's February 21, 2021, letter to NIST on the agency's four draft publications on IoT device cybersecurity for federal agencies.

[9] 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