U.S. Chamber of Commerce

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

October 6, 2023

Via https://www.fcc.gov/ecfs/filings/standard

Marlene H. Dortch
Secretary
Federal Communications Commission
45 L Street, NE
Washington, DC 20554

Re: Cybersecurity Labeling for Internet of Things: Proposed Rule; PS Docket No. 23–239 (*Federal Register*, August 25, 2023)

Dear Ms. Dortch:

The U.S. Chamber of Commerce welcomes the opportunity to comment on the Federal Communications Commission's (the FCC's or the Commission's) proposed rule on Cybersecurity Labeling for Internet of Things (IoT),[1] including the short extension of the comment and reply comment periods.[2]

For several years, the Chamber has advocated for the development, sales, and use of strong IoT in public and private markets. We appreciate the White House's efforts this summer to encourage leading electronics and appliance manufacturers and retailers to make voluntary commitments to increase the cybersecurity of smart devices and help consumers choose products that are less vulnerable to cyberattacks.[3]

I. Remarkable Progress Is Being Made Toward Strengthening IoT Cybersecurity

The Chamber is an important leader in public-private efforts to enhance IoT cybersecurity. Worth highlighting, in February 2019, the Chamber and 23 other associations sent a letter to the White House urging the administration and Congress to back a National Institute of Standards and Technology (NIST) partnership with industry to strengthen IoT cybersecurity. We noted that NIST would be uniquely suited to convene a public-private effort to "identify a flexible, performance-based, and cost-effective approach that can be voluntarily used by producers, sellers, and users of IoT devices to help them manage cyber risks, data, and privacy."[4]

In addition, the Chamber testified before Congress on IoT cybersecurity; collaborated with NIST in crafting NIST interagency report 8259 (NISTIR 8259);[5] and worked closely with Congress on the Internet of Things Cybersecurity Improvement Act of 2020 (the IoT Act), which sets cybersecurity requirements for federal devices that are connected to the internet.[6]

Industry and NIST have taken significant steps to strengthen cybersecurity for all new IoT devices, and the Chamber urges the Commission not to disrupt such guidance and foundational practices, including through the FCC's proposed rule. The Chamber urges the Commission to track closely with public-private developments in IoT cybersecurity as well as industry-driven initiatives, such as the *C2 Consensus on IoT Device Security Baseline Capabilities* (C2 Consensus) and CTIA's cybersecurity certification program for IoT devices.[7]

In September 2021, eight leading communications and technology industry associations, led by the Consumer Technology Association (CTA), wrote to the Commission to explain that these initiatives have led to tangible, positive impacts on product development, enterprise and retail sales, and IoT deployments and should not be hindered by the creation of new cybersecurity mandates.[8] The Chamber supported the March 2021 CTA-led white paper *Smart Policy to Secure our Smart Future: How to Promote a Secure Internet of Things for Consumers (Smart Policy)*, which promoted public-private partnerships to develop and deploy risk-based approaches to cybersecurity rather than prescriptive regulation.[9]

The Chamber does not attempt to address the multiple points and questions raised in the Commission's proposed rule, and we intend to submit reply comments on November 10. In this letter we emphasize key themes that have been fundamental to Chamber thinking on IoT cybersecurity, which we urge the administration, the Commission, and Congress to adopt. Meanwhile, the Commission should look to the Chamber as a resource as officials continue their work on IoT labeling.

We have reservations about the apparent scope of the Commission's work. The FCC could easily make a labeling initiative overly complicated, specifically by mandating certain IoT capabilities rather than working with industry to decide on a menu of acceptable standards for protecting IoT. Next it should craft a workable conformance program in collaboration with industry. Following this, the Commission should grant a safe harbor to the manufacturers, the sellers, and the users of labeled IoT. If the Commission wants this labeling program to be successful, these three things need to be prioritized above other initiatives.

Decide on acceptable standards.

Develop workable conformance program.

Safeguard labeled IoT and businesses

II. The Commission Should Interpret Its Authority to Set Requirements With Humility

The Commission believes that it has authority to adopt the proposed IoT labeling program. The Commission states that the Communications Act of 1934 authorizes it to make "reasonable regulations" governing the "interference potential of devices[,] which in their operation are capable of emitting radio frequency energy by radiation, conduction, or other means in sufficient degree to cause harmful interference to radio communications."[10]

The Commission adds that participating entities would "need to do so in accordance with *the regulations the Commission adopts in this proceeding, including but not limited to the IoT security standards, compliance requirements, and the labeling program's operating framework*" [italics added]. In short, the Commission seems to contend that it may administer the proposed IoT labeling program because its authority falls within the scope of reasonable regulations that govern the interference potential of devices.

The Chamber is concerned with the Commission's interpretation of its legal authority. First, the FCC's claim of legal authority would, in practical terms, mean that the agency is making policy and regulations and establishing an enforcement regime for the entire federal government regarding IoT cybersecurity. Second, the Chamber is concerned that pursuing such sweeping authority to regulate IoT device cybersecurity would create a problematic precedent to utilize the Commission's harmful interference authorities as a broad regulatory tool.

A firm told the Chamber, "The Commission should build on the good work that government and business have already accomplished, which Commission leaders highlight,[11] and not misread its authority and set granular security requirements across all IoT. Appropriate best practices and standards exist or are being developed. Above all, the Commission should reach a consensus with industry on fundamental concerns including the scope of covered IoT, security criteria and standards, conformity assessments, and liability protections. The mechanics of the labeling program are important, but these other issues need to be settled first." Further, the extensive and lengthy challenges associated with the Defense Department's Cybersecurity Maturity Model Certification program should prompt the Commission to develop its labeling program with humility.[12]

The Chamber believes that the Commission should not overinterpret its harmful interference authority under sections 302(a) and 333 to regulate the cybersecurity of IoT.[13] Many stakeholders have expressed skepticism about the Commission's legal authority to take the actions contemplated in the proposed rule. To date, the Commission has not played a role in reviewing IoT for cybersecurity risks, and Congress did not look to the Commission when it considered and passed legislation to improve IoT cybersecurity.[14]

If the Commission pursues IoT regulation under a labeling program, it needs to be careful to avoid adding to the policy, legislative, and regulatory fragmentation that IoT stakeholders already face in the U.S. and internationally. Instead of exacerbating the mix of cybersecurity requirements, Commission leaders should contemplate creative ways to both streamline regulations and safeguard parties that build, sell, and deploy labeled IoT.

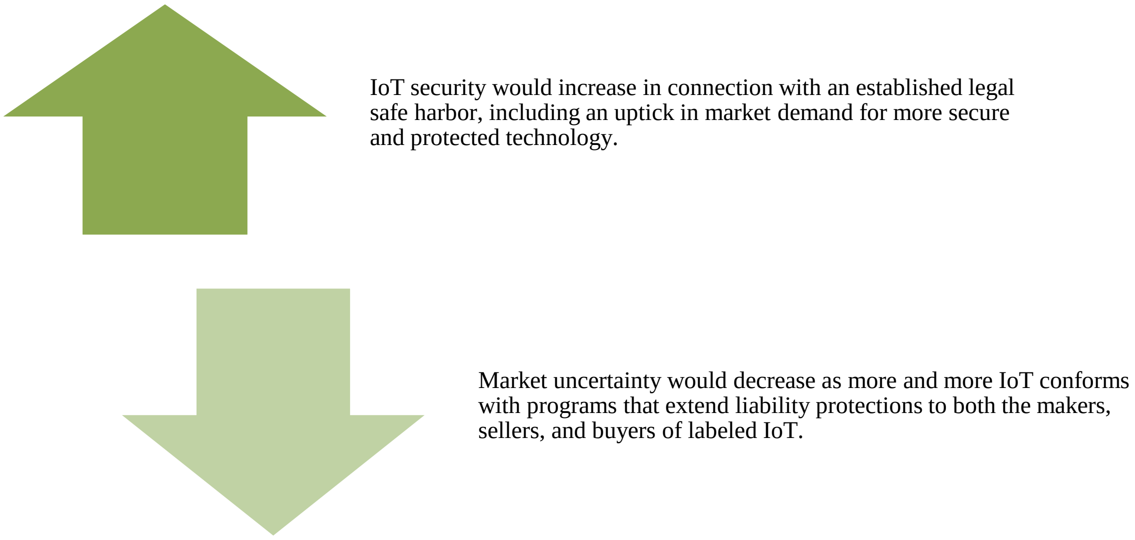
III. Protections and Preemption Are Missing From the FCC's Proposal

For a number of years, the Chamber has maintained that legislation is preferable to agency action because, among other things, proposals like the Commission's lack protections and preemption—two industry priorities. The Chamber recognizes that the Commission cannot write and pass legislation. Yet simply commenting on the proposed rule overlooks the big picture, including the role that agencies and Congress should play in discussions on IoT cybersecurity.

The Chamber has argued that Congress should pass a federal, preemptive law that both addresses IoT cybersecurity and extends legal liability protections to industry. Such a law would have the benefits of giving policymakers, the business community, and consumers more of what they need.[15] The Chamber holds that IoT security would increase in connection with an established legal safe harbor, including an increase in demand for more secure devices and products. Market uncertainty, which the Commission is responding to, would decrease as more and more IoT conform with programs that extend liability protections to the makers, sellers, and buyers of labeled technology.

The Commission is one actor, albeit an important one, in the IoT policy space. Fragmented policy approaches to IoT cybersecurity are likely to 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.

Increased Product Security Would Reduce Market Uncertainty



IoT 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 conforms with programs that extend liability protections to both the makers, sellers, and buyers of labeled IoT.

After all, the administration is seeking ways to increase the presence of more securable IoT 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 shorthand way to think about the Chamber's approach is to summarize it in three words—program, protection, and preemption.

PROGRAM

The Chamber strives to collaborate with policymaking bodies, such as the FCC, to strengthen the cybersecurity environment for governments, businesses, and consumers. We are especially interested in advancing innovative cybersecurity policies 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.

It is critical for the Commission to understand that the Chamber believes that 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. Also critical, policy should offer private parties a range of appropriate standards, guidelines, and frameworks to select from, facilitating choice and the buy-in of parties that may be subject to various regulatory requirements or expectations.[16]

Relatedly, programs should establish reciprocity requirements to better harmonize laws, regulations, and other obligations. Congressionally created programs, the Chamber contends, 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.

The Key to Security and Conformance Is Flexibility in the Choice of Standards

The Commission is seeking feedback on how IoT can demonstrate compliance with the security standards once they are developed. It proposes that conformity for IoT be based on a compliance assessment that includes supporting documentation and data submitted by the manufacturer or importer of the IoT in question to a third party.[17]

Many businesses told the Chamber that the Commission's "voluntary" IoT labeling program would eventually become both mandatory and prescriptive. The Chamber is willing to give the Commission the benefit of the doubt. We, too, support the widespread production and use of strong IoT. In contrast, a prescriptive program would quickly upend the Commission's goal of making IoT more secure. A compliance mindset would water down industry's incentives to meet rigorous standards even if newer or other standards are better. Businesses, we contend the Commission agrees, should be directing resources to where they're needed based on the security challenges and attack surfaces that an IoT faces.

While far from a comprehensive listing, policymakers should deem that the following cybersecurity best practices, frameworks, standards, and programs satisfy the IoT security standards and testing requirements. What is particularly important is that the federal government, including the FCC, should not impose its own criteria or standards on IoT. Policy should spotlight a range of flexible options for stakeholders to choose from based on the IoT's wide range of device complexity, deployment environments, use cases, and risk profiles.[18]

The FCC Should Foster a Diverse Selection of Industry-Driven Best Practices and Standards

To create a workable IoT labeling program, the Commission should promote industry-driven best practices and international standards given the versatile and dynamic nature of the IoT ecosystem. A flexible approach, leveraging cutting-edge practices and standards, can support a broader, scalable implementation of IoT security across the public and private sectors and spur innovation.

A labeling program should offer businesses a range of appropriate standards, guidelines, and frameworks to select from, which would facilitate choice and the buy-in of parties that may be subject to a conformity assessment. The Commission should eschew establishing a prescriptive IoT security labeling regime, which, among an array of challenges, would be difficult to administer.[*] Voluntary labeling approaches should be driven by industry, informed by risk-management principles, and tailored to specific contexts.[19] There are multiple resources for manufacturers, network operators, and enterprises to consider. Here are some examples:[20]

- ANSI/CTA 2088.[21]
- The C2 Consensus on IoT Device Security Baseline Capabilities.[22]
- CableLabs Gateway Device Security Best Common Practices.[23]
- CTIA—The Wireless Association IoT Cybersecurity Certification.[24]
- ETSI 103 645.[25]
- EU Agency for Cybersecurity Baseline Security Recommendations for IoT.[26]
- GSMA IoT Security Guidelines for Endpoint Ecosystems.[27]
- ISO/IEC 27402.[28]
- UK DCMS Code of Practice for Consumer IoT Security.[29]
- UL MCV 1376—Security Capabilities Verified.[30]

[*] The *Profile of the IoT Core Baseline for Consumer IoT Products* (NISTIR 8425) is worth quoting at length: "[S]pecific standards, solutions, implementations, or mitigations should be used as appropriate for an IoT product's functionality and use case. This means no single set of specific requirements can be applicable to all consumer IoT products. Therefore, the consumer profile describes IoT product-level cybersecurity guidelines in terms of outcomes to be achieved and supported by the product as a whole but may not apply to all IoT product components the same way. Some components may not be able, or need, to support all criteria. These outcomes provide guidance for a variety of technologies and use cases but allow flexibility in the application of the consumer profile to specific IoT products" (p. 21).
https://csrc.nist.gov/pubs/ir/8425/final
https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8425.pdf

PROTECTION

The Chamber welcomes the Commission's interest in extending liability protections to labeled IoT. The proposed rule asks—

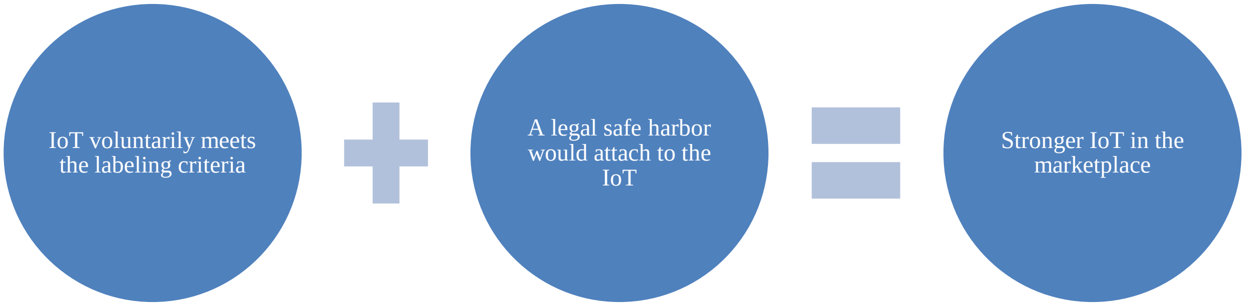
Where a program participant has "received authorization to utilize the Commission's IoT label" and has "appropriately maintained the device's security measures," would this reasonably serve as a "defense or safe harbor against liability for damages resulting from a cyber incident" (e.g., a data breach or a denial of service attack)?[31] The Chamber strongly believes that the answer is yes.

Businesses contend with relentless, often state-sponsored, cyberattacks but frequently lack effective government protection. This widening security gap justifies blending new cybersecurity requirements with regulatory and legal protections. The Commission can respond by granting legal liability protections to organizations that take additional steps to elevate IoT cybersecurity. Depending on the nature of a labeling program, legal liability protections could 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. (See Appendix.)

The Chamber is concerned about labeling and certification programs related to cybersecurity, including their costs. There is no public-private consensus that labeling is a silver bullet even if labels empower consumers to make decisions based on security. Indeed, if policymakers are confident that labeling and certification programs would deliver the security and resilience that these programs suggest, then labels and certifications should be paired with legal liability protections for the producers, sellers, and users of stronger IoT. Authorizing legal liability protections for industry would be a sure way to bolster the presence of trusted IoT equipment on U.S. networks and information systems.

A Win-Win for All Stakeholders: A Safe Harbor Would Lead to Stronger IoT in the Marketplace

The working model that the Chamber envisions provides a blueprint for policymakers to encourage businesses to invest in IoT cybersecurity, which would 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 nonregulatory action, which is consistent with the aims of the Commission and the administration.


IoT voluntarily meets the labeling criteria
A legal safe harbor would attach to the IoT
Stronger IoT in the marketplace

The Chamber sent two letters to NIST, one in October and one in December 2021, regarding the agency's proposed baseline cybersecurity criteria for consumer IoT devices. In many respects, these two letters help address the Commission's request for public input on issues such as potential incentives for implementing a consumer labeling scheme based on NIST recommendations.[32]

In these letters, the Chamber stresses our concern with cybersecurity labeling and/or certification programs, including their costs, absent some offsetting program. If policymakers believe that labeling programs would deliver the cybersecurity benefits that these efforts suggest, then labels should be confidently paired with legal liability protections for the producers, the sellers, and the users of stronger consumer IoT products and software. In addition, the Chamber believes that private-sector administrators or accreditors of labeling and certification programs should also receive legal liability protections.

The administration and the Commission seek ways to increase the presence of more securable IoT 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 mandates 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 abroad.

NIST included the Chamber's concerns about legal liability in the agency's report to the White House on cybersecurity labeling for consumer software and IoT devices.

Report to the White House on Cybersecurity Labeling for Consumers:
Internet of Things (IoT) Devices and Software (Selected Excerpts)
May 10, 2022[33]

Cybersecurity Criteria for Consumer Software

Challenges were cited with end-of-life/expiration dates for software. Feedback was consistent that a label should convey to the consumer if, and for how long, a piece of software would receive security-related updates. However, industry stressed that making such claims could negatively influence industry participation due to liability concerns. NIST addressed those potentially conflicting views by including criteria that allowed consumers to make informed decisions regarding longevity of software and permitted manufacturers flexibility in making support claims. (p. 5)

Cybersecurity Labeling Pilots

Manufacturers, software developers, retailers, and others that participate in future labeling efforts would likely be taking on liability, even if these programs are voluntary. Those liability challenges were said to include having labels misconstrued as warranties and label statements misattributed as endorsements by digital storefronts and retailers. Moreover, stakeholders posited that without adequate legislative/regulatory protections, participation in labeling programs would likely suffer, despite being voluntary. (p. 8)

Conclusions

The liability of key stakeholders throughout the ecosystem may discourage the voluntary adoption of a cybersecurity label. Liability protections for scheme owners and other scheme participants must be addressed by government, perhaps through legislative or regulatory actions. (p. 9) [Bolding in the original; underlining added.]

Preemption. The Commission notes in its proposed rule that "it does not intend at this time for the labeling program in and of itself to preempt otherwise existing law." However, the proposal asks whether "there [are] other affirmative measures that the Commission should consider adopting that should be afforded to devices that have achieved and maintained a Commission IoT security label?"[34]

The Commission can help mitigate the increasing policy fragmentation by enabling businesses to comply with a diverse mix of innovative practices and international standards and not making the choice for them. As new cybersecurity laws continue to be enacted domestically and internationally, businesses are forced to navigate a crowded patchwork of obligations. Adopting a flexible and risk-based labeling policy would better enable business entities to funnel scarce resources toward significant cybersecurity risks.

The optimal approach forward is for Congress to 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.

***

Thank you for the opportunity to provide the Commission with comments on the IoT labeling proposal. If you have any questions or need more information, please do not hesitate to contact Matthew Eggers (meggers@uschamber.com).

Sincerely,

Matthew J Eggers

Matthew J. Eggers
Vice President
Cyber, Space, and National Security Policy Division
U.S. Chamber of Commerce

Appendix

The Commission Is Urged to Back the *National Cybersecurity Strategy's* (NCS') Call for an IoT Security Safe Harbor

The Commission seeks comment on "the process for assessing conformity of consumer IoT" under the labeling program, including self-attestations and third parties.[35] First, it is constructive that the White House's NCS calls for an adaptable safe harbor to shield businesses from liability that "securely develop and maintain" products and services such as IoT.[36] The NCS' acknowledgement of the need for a safe harbor is a welcome step.

Second, under the proposed IoT labeling program, IoT producers would be required to attest to their devices' and/or products' compliance with secure IoT development practices. Such attestations should come with liability protections based on the level of certification or conformity that an IoT producer undertakes. It is reasonable that the Commission should authorize a safe harbor for IoT when it meets certain cybersecurity requirements.

Third, neither industry nor government should receive a public policy free lunch. Without a doubt, businesses bear the significant costs associated with nefarious cyber activity led by criminal organizations and nation-states. If the Commission believes that the compliance requirements would deliver the security benefits that the labeling program suggests, officials should confidently pair adherence to standards and so forth identified under the labeling program with liability protections.

Policymakers should stand behind the perceived correctness of their regulations. Anything short of clear liability protections for IoT producers would call into question the assumption that the cybersecurity requirements are appropriately risk based, technically sound, and workable.

	Self-attestation (voluntary)	**Third-party assessment (voluntary or mandatory)**
Type of liability protection	*Affirmative defense* against agency penalties or certain causes of action arising from a cyber incident tied to labeled IoT.	*Indemnification* against agency penalties or certain causes of action arising from a cyber incident tied to labeled IoT.
Type of cybersecurity program	Standards etc. identified under the labeling program.	Standards etc. identified under the labeling program.

Notes

[1] FCC proposed rule on Cybersecurity Labeling for Internet of Things, *Federal Register* (*FR*), August 25, 2023. https://www.federalregister.gov/documents/2023/08/25/2023-18357/cybersecurity-labeling-for-internet-of-things

[2] *FR*, September 26, 2023. https://www.federalregister.gov/documents/2023/09/26/2023-20921/cybersecurity-labeling-for-internet-of-things

[3] The White House, "Biden-Harris Administration Announces Cybersecurity Labeling Program for Smart Devices to Protect American Consumers," July 18, 2023. https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/18/biden-harris-administration-announces-cybersecurity-labeling-program-for-smart-devices-to-protect-american-consumers

[4] https://www.uschamber.com/assets/archived/images/2-7-19_multi-association_wh_letter_iot_cybersecurity_final.pdf

[5] For example, see:

Testimony on Cybersecurity of the Internet of Things before the House Oversight and Government Reform Committee Information Technology Subcommittee, October 3, 2017.
https://www.govinfo.gov/app/details/CHRG-115hhrg27760/CHRG-115hhrg27760
https://republicans-oversight.house.gov/wp-content/uploads/2017/10/Eggers_Testimony_IOT_10032017.pdf

NIST IoT Cybersecurity Colloquium, October 19, 2017.
https://www.nist.gov/news-events/events/2017/10/iot-cybersecurity-colloquium
https://www.nist.gov/system/files/documents/2017/10/23/mattheweggers_slides.pdf

Testimony on Strengthening the Cybersecurity of the Internet of Things before the Senate Commerce Committee Security Subcommittee, April 30, 2019.
https://www.commerce.senate.gov/2019/4/strengthening-the-cybersecurity-of-the-internet-of-things
https://www.commerce.senate.gov/services/files/7C13BC4E-64C2-4EB3-9F3B-9B9872EB44D7

Letter to NIST on draft NISTIR 8259, the core cybersecurity baseline for IoT device makers, September 2019.
https://www.uschamber.com/sites/default/files/09-30-19_uscc_comment_letter_nistir_8259_final_v1.0.pdf

Letter to NIST on 2nd draft of NISTIR 8259, February 2020.
https://www.uschamber.com/sites/default/files/200211_uscc_comments_nistir_8259_second_draft_final.pdf

Letter to NIST on draft guidance on federal IoT cybersecurity (federal profile), February 2021.
https://www.uschamber.com/sites/default/files/2-26-21_uscc_comments_nist_iot_cyber_fed_profile_final_v1.0.pdf

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

[7] In September 2019, the Chamber wrote NIST to express support for NISTIR 8259. We also expressed backing for the C2 Consensus. The Chamber participated in the creation of the C2 Consensus baseline, led by the Council to Secure the Digital Ecosystem (CSDE). The C2 Consensus provides experienced guidance to the public and private sectors on securing new IoT devices to raise the market's expectations for security and advance policy harmonization globally. C2 Consensus parties expect that this orientation toward international harmonization would enhance security more effectively compared with a number of troubling regional or local initiatives that industry is witnessing domestically and overseas.
https://csde.org/projects/c2-consensus
https://ctiacertification.org/program/iot-cybersecurity-certification

[8] See the September 2021 letter to the FCC from ACT | The App Association; Consumer Technology Association; CSDE; CTIA—The Wireless Association; Internet Association; Information Technology Industry Council; Telecommunications Industry Association; and USTelecom—The Broadband Association.
https://www.fcc.gov/ecfs/filing/1092055130384

[9] https://www.cta.tech/Resources/Newsroom/Media-Releases/2021/March/IOT-Device-Security-White-Paper-Release

[10] *FR*, pp. 58221–58222.

[11] See the statements of Chairwoman Jessica Rosenworcel and Commissioner Geoffrey Starks.
https://www.fcc.gov/document/fcc-proposes-cybersecurity-labeling-program-smart-device
https://docs.fcc.gov/public/attachments/FCC-23-65A2.pdf
https://docs.fcc.gov/public/attachments/FCC-23-65A3.pdf

[12] Justin Doubleday, "Congressional auditors point to challenges ahead for Pentagon's CMMC program," *Federal News Network*, December 10, 2021.
https://federalnewsnetwork.com/defense-main/2021/12/congressional-auditors-point-to-challenges-ahead-for-pentagons-cmmc-program

[13] 47 U.S.C. § 302a, "Devices which interfere with radio reception."
https://www.law.cornell.edu/uscode/text/47/302a

47 U.S.C. § 333, "Willful or malicious interference."
https://www.law.cornell.edu/uscode/text/47/333

[14] See the Chamber's October 2021 reply comments to the FCC on the proposed rule on Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program, *FR*, August 19, 2021. The Commission sought comments on how to leverage its equipment authorization program to encourage manufacturers that are building devices that will connect to U.S. networks to consider cybersecurity standards and guidelines.
https://www.fcc.gov/ecfs/search/search-filings/filing/10182049018274
https://www.fcc.gov/ecfs/document/10182049018274/1
https://www.federalregister.gov/documents/2021/08/19/2021-16087/protecting-against-national-security-threats-to-the-communications-supply-chain-through-the

[15] In December 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.

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.

[16] The 2018 Ohio Data Protection Act (S.B. 220) is a notable model that the Chamber supports. Ohio enacted this innovative data security/cybersecurity 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/sites/default/files/2021-12/cybersecurity-whitepaper-32819F-1.pdf
https://moritzlaw.osu.edu/faculty-and-research/program-data-and-governance/program-data-and-governance-research-publications

[17] *FR*, p. 58218.

[18] *Smart Policy*, p. 6.

[19] Ibid, p. 11.

[20] Ibid, pp. 6–7.

[21] https://standards.cta.tech/apps/group_public/project/details.php?project_id=594
https://www.nist.gov/system/files/documents/2021/09/03/CTA%20Position%20Paper%20on%20Cybersecurity%20Label%20Considerations%20Final.pdf

[22] https://csde.org/projects/c2-consensus

[23] https://www.cablelabs.com/blog/raising-the-bar-on-gateway-device-security
https://www.cablelabs.com/specifications/CL-GL-GDS-BCP

[24] https://ctiacertification.org/program/iot-cybersecurity-certification

[25] https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/02.01.02_60/ts_103645v020102p.pdf

[26] https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

[27] https://www.gsma.com/iot/iot-security-guidelines-for-endpoint-ecosystem

[28] https://www.iso.org/standard/80136.html

[29] https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security

[30] https://www.ul.com/news/uls-iot-security-rating-helps-demonstrate-product-security-marketplace
https://www.shopulstandards.com/Catalog.aspx

[31] *FR*, p. 58221.

[32] See the Chamber's October 20, 2021, letter to NIST on the agency's draft *White Paper on Baseline Security Criteria for Consumer Internet of Things (IoT) Devices*.
https://www.nist.gov/system/files/documents/2021/10/29/37-US%20Chamber%20Comments_DraftCriteria_IoTLabeling_NIST.pdf

https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/comments-received-draft-consumer-labeling-iot
https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/iot-product-criteria

See the Chamber's December 16, 2021, letter to NIST on the agency's draft *Baseline Criteria for Consumer Software Cybersecurity Labeling*.
https://www.nist.gov/system/files/documents/2022/01/18/Chamber_211216_Comments_SW-IoTLabeling_NIST.pdf
https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/comments-received-draft-baseline-criteria
https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/consumer-software-criteria

Under Executive Order (EO) 14028, Improving the Nation's Cybersecurity, NIST was called on to consider two labeling programs related to the cybersecurity of consumer IoT products and software. The order also directs NIST to account for existing consumer product labeling programs as it assesses what efforts may be needed to educate the public on the cybersecurity capabilities of IoT products and software.
https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/consumer-cybersecurity-labeling-pilots-approach

[33] See the Chamber's March 14, 2022, comments on consumer cybersecurity labeling pilots, which the White House calls for under EO 14028, *Improving the Nation's Cybersecurity*.

NIST, *Consumer Cybersecurity Labeling Pilots: The Approach and Contributions*, February 2022. https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/consumer-cybersecurity-labeling-pilots

NIST, *Report for the Assistant to the President for National Security Affairs (APNSA) on Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software: A summary review of labeling actions called for by EO 14028: Improving the Nation's Cybersecurity*, May 10, 2022. https://www.nist.gov/system/files/documents/2022/05/24/Cybersecurity%20Labeling%20for%20Consumers%20under%20Executive%20Order%2014028%20on%20Improving%20the%20Nation%27s%20Cybersecurity%20Report%20%28FINAL%29.pdf

[34] *FR*, p. 58221.

[35] *FR*, pp. 58217–58218.

[36] NCS, March 2023, p. 21. The NCS calls for rebalancing responsibilities for cybersecurity away from individuals, small businesses, and local governments and toward the organizations that are most capable and best positioned to reduce cybersecurity risks. The strategy also calls for realigning incentives to favor long-term investments, including supporting an adaptable safe harbor framework.

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 asserted 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