October 18, 2021

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

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

**Subject: Reply Comments Regarding Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program (Docket No. 21-232)**

Dear Secretary Dortch:

The U.S. Chamber of Commerce appreciates the opportunity to provide the Federal Communications Commission (the FCC or the Commission) feedback on the agency's notice of inquiry (NOI) regarding ways to strengthen Internet of Things (IoT) cybersecurity.[1]

The Chamber agrees with the Commission's view that the development and implementation of effective cybersecurity practices require the "continued cooperation and participation of all stakeholders." The Commission notes that "both the public and private sectors have come together to develop measures to protect the integrity of communications networks and guard against malicious or foreign intrusions that can compromise network services, steal proprietary information, and harm consumers." The agency further notes that the National Institute of Standards and Technology (NIST) has worked with both industry and government to "produce multiple cybersecurity frameworks and other forms of guidance that help protect the integrity of communications networks."[2]

The Chamber is particularly pleased with the work that the business community and NIST have jointly undertaken to prioritize IoT cybersecurity and create workable approaches to enhancing IoT cybersecurity for both U.S. and international stakeholders. As the Commission examines the next steps concerning its NOI and notice of proposed rulemaking (NPRM),[3] the Chamber urges the FCC to take our perspectives into account.

**Summary**

- The Chamber agrees with the Commission's view that the public and private sectors have collaborated well in developing measures to defend U.S. communications networks and guard against malicious activity undertaken by foreign nations or their proxies. Over the past few years, remarkable progress has been made toward strengthening IoT cybersecurity.

- The Chamber urges the Commission to lend its weight to ongoing industry and NIST efforts to advance market-driven standards and certification tools rather than using its equipment authorization regime to regulate IoT cybersecurity. Otherwise, the FCC would add to the policy, legislative, and regulatory fragmentation that IoT device stakeholders confront in the U.S. and globally.

- The Chamber believes that Congress should pass a federal, preemptive law that both addresses IoT cybersecurity and extends legal liability protections to industry.

- Government-driven certification and/or labeling programs related to cybersecurity are no silver bullet. If policymakers are confident that federally directed certification and/or labeling regimes would deliver the cybersecurity that these programs tend to presume, then they should be paired with legal liability protections for producers, sellers, and users of stronger IoT devices.

**Substantial Progress Is Being Made Toward Strengthening IoT Cybersecurity**

The Chamber has been 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 NIST's partnership with industry to strengthen IoT cybersecurity. The letter called on policymakers to support NIST in convening a robust effort on IoT security and resilience. Such an initiative, the organizations argued, will help stakeholders 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 risk and threats.[4] To date, this public-private effort is proceeding well and producing tangible results.

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]

The Chamber maintains that industry and NIST have taken significant steps to strengthen cybersecurity for all new IoT devices, and we urge the Commission not to disrupt such guidance and foundational practices, including through the FCC's equipment authorization program. The Chamber strongly urges the FCC 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]

On September 20, 2021, eight leading communications and technology industry associations, led by the Consumer Technology Association (CTA), wrote to the FCC 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 welcomes the March 2021 CTA-led white paper, *Smart Policy to Secure our Smart Future: How to Promote a Secure Internet of Things for Consumers*, which promotes public-private partnerships to develop and deploy risk-based approaches to cybersecurity rather than top-down regulation.[9]

**FCC Regulation of IoT Device Security Would Add to a Growing List of Government Requirements**

The Chamber believes that the Commission should not use its equipment authorization regime to regulate the cybersecurity of internet connected devices. We agree with the associations' letter to the FCC, which raises questions about the Commission's legal authority to regulate IoT device security. The organizations argue that "[t]here are significant doubts about the FCC's legal authority to take the actions contemplated in the NOI. To date, the FCC has not played a role in reviewing devices for cybersecurity risks, and Congress did not look to the FCC when it considered and passed legislation to improve IoT cybersecurity."[10]

The associations go on to say that "FCC regulation of the security of connected devices would venture far beyond the role given to it by Congress in equipment authorization," which has been focused on matters such as radiofrequency emissions and spectrum use. The associations add that while the Commission has identified the Secure Networks Act as "a potential source of authority for the limited actions proposed in the NPRM," the Secure Networks Act does not enable the FCC to "engage in a wide-ranging inquiry into cybersecurity writ large." Similarly, the Chamber believes that the FCC's initial conclusion that regulating the security of IoT devices "is not specifically authorized by the Secure Networks Act itself" is correct.[11]

If the Commission were to pursue regulating the cybersecurity of IoT devices, the FCC would add to the policy, legislative, and regulatory fragmentation that IoT device stakeholders already face in the U.S. and internationally. Instead of exacerbating the thicket of cybersecurity requirements, Commission leaders should work toward streamlining them.

**The Solution: 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 Commission 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.[12] 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.[13]

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 Commission's NOI specifically requests feedback on government certification and/or labeling of IoT devices. The timing of this questioning is helpful because it relates to a directive in the White House's Executive Order (EO) *Improving the Nation's Cybersecurity*.[14]

Section 4 of the EO 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. NIST is also directed 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.[15] While this review by NIST is underway, the Chamber contends that regulatory pursuits, including by the FCC, should not be undertaken.

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.[16] 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.

**Securable Devices Need to Be Built and Bought**

The impressive work undertaken by NIST and the C2 Consensus may not be fully realized without a clear and growing demand for securable devices. Market demand is growing, but it needs to be cultivated.[17] More securable IoT technologies need to be designed, built, and bought. To achieve this objective, the Chamber envisions a broad array of stakeholders promoting the production, purchase, and deployment of more secure IoT products across the U.S. and globally. Simply put, the Chamber wants device makers, service providers, and buyers

to benefit from the business community leading the development of state-of-the-art IoT components and sound risk management practices to improve the security and resilience of the emerging IoT ecosystem.

**U.S. and International Policies Need to Be Aligned to the Baseline**

The Chamber supports efforts that spur commercial demand for strong devices by consumers, such as public and private enterprises and households. Policymakers at home and abroad need to align their IoT cybersecurity policies to the industry-led baseline. There is a robust consensus that IoT cybersecurity efforts will be most effective if they reflect global standards and innovative commercial practices, especially *NISTIR 8259* and the C2 Consensus.

The Chamber welcomes the opportunity to provide the Commission comments on the NOI. 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 Supply Chain Security

Matthew J. Eggers
Vice President, Cybersecurity Policy

Endnotes

[1] Federal Communications Commission, "Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program and the Competitive Bidding Program," *Federal Register* (FR), August 19, 2021. In sum, the notice says, "The Commission seeks comment on how to leverage its equipment authorization program to encourage manufacturers who are building devices that will connect to U.S. networks to consider cybersecurity standards and guidelines."
https://www.federalregister.gov/documents/2021/08/19/2021-16087/protecting-against-national-security-threats-to-the-communications-supply-chain-through-the

[2] FR p. 46642.

[3] The Chamber joined a multi-association letter on the proposed rulemaking.
https://ecfsapi.fcc.gov/file/1092006509962/Industry%20Letter%20NPRM.pdf

[4] In February 2019, the Chamber and 23 associations sent a letter to the White House urging the administration and Congress to support the National Institute of Standards and Technology's (NIST's) efforts alongside industry to bolster IoT cybersecurity.

https://www.uschamber.com/sites/default/files/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

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 *NIST interagency report 8259 (NISTIR 8259)*, the core cybersecurity baseline for IoT device makers, September 30, 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 11, 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 26, 2021.
https://www.uschamber.com/sites/default/files/2-26-21_uscc_comments_nist_iot_cyber_fed_profile_final_v1.0.pdf

[6] The Internet of Things Cybersecurity Improvement Act of 2020 (P.L. 116-207), or the IoT Act.
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 will 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 20, 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
https://ecfsapi.fcc.gov/file/1092055130384/Industry%20Letter%20NOI.pdf

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

[10] The IoT Act.

[11] FR p. 46643.

H.R. 4998, the Secure and Trusted Communications Networks Act of 2019 (P.L. 116-124)
https://www.congress.gov/bill/116th-congress/house-bill/4998

[12] 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

[13] 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

[14] 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

[15] 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

[16] 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

[17] The November 2019 *Botnet Road Map* calls for establishing robust markets for consumer and industrial devices.
www.ntia.doc.gov/blog/2018/road-map-building-more-resilient-internet