Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Protecting Against National Security Threats	)	ET Docket No. 21-232
to the Communications Supply Chain through the	)	EA Docket No. 21-233
Equipment Authorization Program and the	)	
Competitive Bidding Program	)	

COMMENTS OF THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

September 20, 2021

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Protecting Against National Security Threats	)	ET Docket No. 21-232
to the Communications Supply Chain through the	)	EA Docket No. 21-233
Equipment Authorization Program and the	)	
Competitive Bidding Program	)	

COMMENTS OF THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

INTRODUCTION AND SUMMARY

The Telecommunications Industry Association ("TIA")[1] respectfully submits these comments in the above-captioned proceedings.[2] TIA represents the global manufacturers and vendors of trusted ICT equipment and services that empower communications networks worldwide. Our members work to leverage modern global supply chains that have been enabling operations across all segments of the global economy and share the Commission's interest in ensuring that all equipment forming the foundation of U.S. ICT networks comes from trusted manufacturers and suppliers. TIA has been active in dockets before the Commission arguing for

[1] TIA is the leading trade association for the information and communications technology ("ICT") industry, representing companies that manufacture or supply the products and services used in global communications across all technology platforms. TIA represents its members on the full range of policy issues affecting the ICT industry and forges consensus on voluntary, industry-based standards.

[2] *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program; Protecting Against National Security Threats to the Communications Supply Chain through the Competitive Bidding Program*, Notice of Proposed Rulemaking and Notice of Inquiry, ET Docket No. 21-232, EA Docket No. 21-233, FCC 21-73 (rel. Jun. 17, 2021) ("NPRM" or "NOI," as appropriate).

the exclusion of equipment from vendors that raise national security concerns, and we have been pleased to see the Commission's actions to date to exclude such equipment in networks funded by the Universal Service Fund ("USF").[3] TIA welcomes the Commission's proposal to take this proceeding to its logical next step and seek input from industry on how the Commission can best mitigate security risks posed by equipment that Congress has identified as presenting risks to U.S. national security.

However, as the FCC proceeds with this rulemaking, TIA suggests that it treat the issues raised in the NPRM and NOI separately so that it may more rapidly confront the national security issues raised in the NPRM. With an administrative record as extensive as that facing some of the Covered Entities, combined with the authority granted to the Commission by Congress, blocking the sale of their equipment in U.S. markets is reasonable.

When it comes to revocation, however, the Commission must not take this extreme step lightly. Before deciding on any action on revocation, it is imperative that the Commission thoroughly weigh the costs of such an action to ICT industry and U.S. consumers and the ubiquitous nature of the equipment that could be revoked against the potential public benefit of such an action. If the Commission then decides to proceed with revocation, it must implement plans to make these parties whole after revoking authorizations for equipment purchased in good faith.

Finally, TIA does not believe the existing equipment authorization and certification process is the appropriate authority or venue for national security and cyber security concerns,

[3] *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Notice of Proposed Rulemaking, 33 FCC Rcd 4058 (2018).

and the FCC must make sure that any new role it may seek to play in security issues does not frustrate ongoing efforts by industry to secure the ICT supply chain.

DISCUSSION

I. THE NPRM AND NOI ADDRESS DIFFERENT PROBLEMS AND THEREFORE THE FCC SHOULD TREAT THEM DISTINCTLY.

At a foundational level, this proceeding plays an important role in protecting the networks of the United States from known threats caused by equipment from certain entities.[4] The NPRM raises this critical concern and proposes to block the authorization and therefore the sale of equipment from U.S. networks that have been shown to present a national security risk. This goal of protecting U.S. networks carries broad industry support, even while the ICT industry may debate about how the Commission should advance this goal. The NOI, on the other hand, presents a broad spectrum of legal questions that need to be properly vetted both with industry and other agencies working on cybersecurity efforts. Some of the questions raised by the NOI, especially as they pertain to the FCC reworking its existing equipment authorization regime to include Internet of Things ("IoT") device security, could have negative consequences for the entire ICT industry.

In fact, the issues raised by the NOI are so far-reaching and nebulous that the FCC might find, after reviewing feedback in this docket, that any further action or rulemaking on the issues raised by the NOI is not practical given the work industry is already engaged in regarding IoT security. But to be clear, the national security concerns related to equipment from Covered Entities pose a clear and present threat to national security, and the FCC should not hold up action on some of the issues raised in the NPRM while it debates its course of action for the

[4] *See infra* § II(b) (discussing the extensive history of Covered Entities, including being specifically named in the 2018 National Defense Authorization Act and the Secure and Trusted Communications Networks Act).

questions raised in the NOI. The FCC should therefore separate the NPRM and NOI into separate proceedings in order to act on the clear national security concerns raised by the Covered Entities and give industry and the Administration time to properly vet the responses in this docket and the legal questions raised by the NOI.

II. THE COMMISSION SHOULD ACT UNDER ITS AUTHORITY FROM THE SECURE AND TRUSTED NETWORK COMMUNICATIONS ACT, AS THE EQUIPMENT AUTHORIZATION PROCESS IS NOT AN APPROPRIATE AUTHORITY FOR SECURITY CONCERNS.

As discussed above, TIA strongly supports the Commission's underlying goal in the NPRM: taking clear and decisive action to ensure that Covered List equipment that poses a clear threat to national security is excluded from the nation's ICT networks and marketplaces. However, the Commission must be sure to take steps to accomplish this goal in a way that would not have unforeseen effects on trusted manufacturers of ICT equipment or consumers of ICT products or frustrate ongoing efforts by both industry and government to secure the ICT supply chain, thus adversely affecting the innovation of trusted ICT equipment.

a. The FCC Should Act to Block Equipment from Covered Entities Under its Clear Authority Granted by Congress.

TIA has been a leading advocate in favor of the Commission taking forceful action against threats posed by Covered Entities since the Commission's first public docket addressing this issue.[5] In fact, dating back to our 2018 comments in the FCC's related "rip and replace" supply chain rulemaking, TIA supported the FCC taking action to remove equipment from Covered Entities from U.S. networks outside of a USF context.[6] TIA believes that the threat to

[5] *See generally* Comments of the Telecommunications Industry Association, WC Doc. 18-89 (Jun. 1, 2018); Reply Comments of the Telecommunications Industry Association, WC Doc. No. 18-89 (Jul. 2, 2018) (*collectively* "2018 Comments"); Comments of the Telecommunications Industry Association, WC Doc. No. 18-89 (Feb. 3, 2020) ("2020 TIA Comments").

[6] *See* 2018 TIA Comments § I(C) (advocating for the Commission to open a Further Notice of Proposed Rulemaking to exclude equipment from suppliers that raise national security concerns).

national security posed by Covered Entities has only become more clear in the public discourse since 2018. It has also become clear that this threat exists whether or not universal service funds were used to purchase the equipment in an ICT network.

TIA does not believe the FCC is lacking the authority to expand a prohibition on equipment from Covered Entities outside of a USF context. On the contrary, TIA has been on record stating that the outcome from the NPRM in this proceeding, the banning of *all* equipment from Covered Entities from U.S. networks, was a "logical outgrowth" of all the work the FCC has been doing the past four years in the USF / Rip and Replace docket. In sum, we believe the FCC has the authority to bar these companies from the U.S. ICT market, and agree with the Commission's goals for this proceeding.

That said, TIA shares the concerns of many in the ICT industry with the idea of grounding this action in the FCC's equipment authorization process for this purpose, and we believe that this is not the appropriate authority for the FCC to act on national security concerns, especially when Congress has already granted the FCC clear authority to act on national security grounds. In 2019, the Secure and Trusted Communications Networks Act ("SNA") passed Congress and was signed into law with the fervent support of TIA.[7] As written, SNA provides the Commission clear authority to act on the underlying goals of the NPRM without disrupting the existing equipment authorization and certification regime.

As the Commission and other commentators are surely aware, SNA was focused on the Rip and Replace effort largely targeted to remove equipment from Huawei and ZTE from USF-funded networks and was already being contemplated by the FCC prior to the passage of the Act. Under Section 2 of SNA, Congress has directed the FCC to publish a list of "any

[7] Secure and Trusted Networks Act of 2019, Pub. L. No. 116-124, 133 Stat. 158 (2020) (codified as amended at 47 U.S.C. §§ 1601-1609) ("Secure Networks Act" or "SNA").

communications equipment or service that poses an unacceptable risk to the national security of the United States or the security and safety of United States persons," based on specific determinations made by Congress or other agencies or interagency bodies named in the statute.[8] While other sections of SNA define additional activities the FCC must take with regard to the reimbursable removal of such equipment from networks subsidized by USF monies, the FCC's duty to list equipment and services that pose an unacceptable risk to U.S. national security exists independently of this replacement program.

The FCC has published this list, which presently includes communications and video surveillance equipment from five such companies, and it possesses the authority under SNA to render such equipment ineligible for authorization under the FCC's equipment authorization process – and thus block such equipment from the U.S. market.[9] Blocking such equipment that poses an "unacceptable risk to the United States" from U.S. markets is a logical, and in our view necessary, step after adding a company to the list required by SNA after making a national security designation. Using SNA as the FCC's main authority for taking this step would also spare a complete reworking of the existing equipment authorization regulations to account for national security concerns, which the existing regime is not currently set up to handle.[10]

This clear authority could be further buttressed by the Secure Equipment Act of 2021 that is currently being debated in both houses of Congress.[11] Similar to SNA, the Secure Equipment Act, which has bipartisan support in Congress, would give express Congressional approval to the current proposals being considered by the FCC, and mandate that the Commission takes action to

[8] 47 U.S.C. § 1601.
[9] These communications and video surveillance companies were first identified by Congress as national security risks in the 2018 National Defense Authorization Act, which was later cited and incorporated by the SNA.
[10] *See infra* § IV(a).
[11] S. 1790 Secure Equipment Act of 2021 (117th Cong.).

ensure that equipment from entities that pose national security concerns is not sold in U.S. markets. The FCC's existing authority to undertake this action would be clarified and thus bolstered by the enactment of the Secure Equipment Act, and TIA urges swift Congressional passage of this legislation.

b. The FCC Should Only Act to Exclude ICT Vendors and Suppliers When Based on an Extensive Record Through a Whole-Of-Government Approach.

TIA and our members have always supported targeted government action when equipment from an entity poses a risk to national security, and we support past steps that have been taken to exclude such equipment from U.S. ICT networks. As we have said in numerous supply chain-related filings, TIA has also always believed that such decisions must come from a whole-of-government approach.[12] It is in the United States' interest to make sure that any action taken by a federal agency against a private company in the name of national security is taken very seriously and bolstered by evidence and determinations from agencies with national security expertise.

As the Commission has discussed throughout its efforts to address national security threats to U.S. communications networks, the record regarding companies that the NPRM seeks to address is extensive and continues to expand. In the decade since the House Permanent Select Committee on Intelligence released its Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE,[13] national security-focused leaders across the U.S. government have voiced concerns about the risk posed by allowing those

[12] *See, e.g.* 2020 TIA Comments § III.

[13] Permanent Select Committee on Intelligence, U.S. House of Representatives, Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE (Oct. 8, 2012), https://republicans-intelligence.house.gov/sites/intelligence.house.gov/files/documents/huaweizte%20investigative%20report%20(final).pdf

companies to participate in U.S. communications supply chains and have initiated a variety of actions in response – a list that has grown even during the pendency of the Commission's supply chain rulemaking and the instant proceedings. Of note, we highlight the following government actions that are roughly coterminous with the FCC's own efforts in this area:

- In December 2017, a group of 18 Senators and Representatives sent a letter to Chairman Ajit Pai highlighting the HPSCI Report's finding that Huawei could not be trusted to be free of foreign state influence and recommending that U.S. government systems and contracts "not include Huawei or ZTE equipment."[14]
- In response to these concerns, Congress passed, and the President signed into law, the National Defense Authorization Act ("2018 NDAA") for Fiscal Year 2018, prohibiting the Department of Defense from using telecommunications equipment or services produced or provided by Huawei or ZTE for certain critical programs.[15] In the 2019 NDAA, Congress and the President went further by prohibiting executive agencies from expending loan or grant funds on "covered telecommunications equipment or services," which it defined as (1) telecommunications equipment produced by Huawei or ZTE or their subsidiaries or affiliates; (2) video surveillance and telecommunications equipment produced by Hytera, Hikvision, or Dahua, or any of their subsidiaries or affiliates; (3) telecommunications or video surveillance services provided by entities using such equipment; or (4) telecommunications or video surveillance equipment provided by an entity otherwise identified by the Secretary of Defense in consultation with the Directors of the National Intelligence or Federal Bureau of Investigation as reasonably believed to be owned, controlled by, or otherwise connected to the People's Republic of China.[16]
- In November 2018, the Department of Homeland Security ("DHS") established the Information and Communications Technology ("ICT") Supply Chain Risk Management Task Force to examine and develop consensus recommendations regarding risks to global ICT supply chains.[17]
- In December 2018, Congress established the Federal Acquisition Security Council through the SECURE Technology Act to develop a government-wide strategy for addressing supply chain risks from ICT purchases, facilitating information sharing to reduce those risks, and establish procedures to remove and exclude suppliers posing a national security threat from federal government systems.[18]
- On May 15, 2019, the President signed Executive Order 13873 on *Securing the Information and Communications Technology and Services (ICTS) Supply Chain*,

[14] Letter from Senator Tom Cotton et al., U.S. Senate, to Hon. Ajit Pai, Chairman, FCC, Dec. 20, 2017, https://apps.fcc.gov/edocs_public/attachmatch/DOC-349859A2.pdf.
[15] Pub. L. 115-91, 131 Stat. 1283, 1762, Sec. 1656.
[16] Pub. L. 115-232, 132 Stat. 1636.
[17] Department of Homeland Security, Press Release, DHS Announces ICT Supply Chain Risk Management Task Force Members (Nov. 15, 2018), https://www.dhs.gov/news/2018/11/15/dhs-announces-ict-supply-chain-riskmanagement-task-force-members.
[18] P.L. 115-390, 132 Stat. 5173, https://www.congress.gov/115/bills/hr7327/BILLS-115hr7327enr.pdf.

declaring a national emergency regarding the acquisition or use of ICTS supplied by entities owned by, controlled by, or subject to the jurisdiction of foreign adversaries.[19]

- On May 16, 2019, the Bureau of Industry and Security ("BIS") amended the Export Administration Regulation to add Huawei and its non-U.S. affiliates to the Entity List due to the U.S. government's determination that there is reasonable cause to believe that Huawei has been involved in activities contrary to the national security or foreign policy interests of the United States.[20]
- On February 13, 2020, the Department of Justice charged Huawei and its subsidiaries with racketeering conspiracy and conspiracy to steal trade secrets, including allegations that Huawei and its subsidiaries were involved in projects in countries subject to U.S., E.U. and/or U.N. sanctions such as Iran and North Korea.[21]
- On June 3, 2021, President Biden signed Executive Order 14032 expanding the scope of the national emergency declared in Executive Order 13959 to prohibit U.S. persons from buying or selling publicly traded securities of listed companies including Huawei and Hikvision.[22]

Congress also directed the Commission specifically to address threats posed by these named suppliers through passage of the SNA and as amended by the Consolidated Appropriations Act ("CAA") of 2021.[23] And, more generally but consistent with all of the above actions, the Biden Administration has signaled its intent to more closely examine supply chains to assess their security.[24]

We support the Commission's significant work to implement these directives born out of the demonstrated and increasing concern and action the U.S. government has taken to address

[19] Executive Order 13873, 84 Fed. Reg. 22689, Executive Order on Securing the Information and Communications technology and Services Supply Chain (May 15, 2019), https://www.whitehouse.gov/presidential-actions/executiveorder-securing-information-communications-technology-services-supply-chain/.
[20] Addition of Entities to the Entity List, 84 Fed. Reg. 22961, (May 21, 2019), https://www.federalregister.gov/documents/2019/05/21/2019-10616/addition-of-entities-to-the-entity-list.
[21] *See* Press Release, Chinese Telecommunications Conglomerate Huawei and Subsidiaries Charged in Racketeering Conspiracy and Conspiracy to Steal Trade Secrets; Charges also Reveal Huawei's Business in North Korea and Assistance to the Government of Iran in Performing Domestic Surveillance (Feb. 13, 2020), https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-subsidiaries-charged-racketeering.
[22] Executive Order 14032, 86 Fed. Reg. 30145, Executive Order Addressing the Threat From Securities Investments That Finance Certain Companies of the People's Republic of China (Jun. 3, 2021), https://www.federalregister.gov/documents/2021/06/07/2021-12019/addressing-the-threat-from-securities-investments-that-finance-certain-companies-of-the-peoples.
[23] Secure Networks Act (2020).
[24] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/.

these concerns over the last decade. Even prior to direction from Congress, the Commission wisely looked to agencies with national security and intelligence expertise to make determinations regarding covered entities. We urge the Commission to continue to employ a whole-of-government approach should any similar action be required in future, and with the benefit of the mechanism laid out in the SNA.[25]

The FCC thus clearly has a substantial record from agencies with national security expertise, as well as the President and acts of Congress, demonstrating the security risks posed by the Covered Entities. Given this extensive record, the Commission's proposal to exclude equipment from these companies is warranted. That said, the FCC should be careful to ensure that its actions on this docket derive directly and "solely" from one or more of the four enumerated authorities in SNA, as opposed to any new authority the Commission might believe it has to make determinations impacting national security.[26]

III. ANY ACTION TO REVOKE EXISTING AUTHORIZATIONS MUST BE THOROUGHLY VETTED GIVEN THE EXTENSIVE SCOPE OF EQUIPMENT AND INCLUDE A MECHANISM FOR REIMBURSING ITS REPLACEMENT.

The Commission has made clear that it views equipment from vendors on the Covered List as a threat to U.S. national security, a determination that is supported by an extensive and well-documented record.[27] The FCC indeed has an important role to continue to play in ensuring

[25] The Secure Networks Act directs the Commission to base its determinations on one or more of the following determinations: (1) a specific determination made by any executive branch interagency body with appropriate national security expertise, including the Federal Acquisition Security Council established under section 1322(a) of title 41; (2) a specific determination made by the Department of Commerce pursuant to Executive Order No. 13873 (84 Fed. Reg. 22689, relating to securing the information and communications technology and services supply chain); (3) the communications equipment or service being covered telecommunications equipment or services, as defined in section 889(f)(3) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232, 132 Stat. 1918); and (4) a specific determination made by an appropriate national security agency). 47 U.S.C. § 1601(c).

[26] *See supra* at II(a).

[27] *See supra* at II(b).

that equipment that poses such national security risks does not undermine the security and reliability of U.S. networks. The Commission has already done extensive work on removing this equipment from networks funded by the Universal Service Fund, but now the NPRM considers the idea of revoking authorizations of Covered Equipment that was already approved for sale in the U.S. ICT market. Such a move would be an extraordinary step, and the FCC is correct to solicit input from industry before making any determination on if, how, and to what extent, it should proceed.

In the NPRM, the Commission asks for comment on to what extent and based on what circumstances it should revoke existing authorizations.[28] In addition to ensuring that the Commission acts only on critical security threats recognized by intelligence experts, it is crucial that the Commission also recognizes the impact revoking these authorizations will have on U.S. companies as any cost-benefit analysis of this rule to ensure that this act is in the public interest. If revocation is truly necessary, then the Commission should utilize input from this proceeding to consider the financial impact of revoking authorizations of equipment from Covered Entities before adopting any rules that include an official revocation of existing authorizations.

While the Commission has dealt with Covered Entities in other proceedings, it should be made clear that the equipment at issue in this proceeding is far broader than the network infrastructure equipment in rural networks the Commission dealt with in the USF Rip and Replace docket. At issue here is not just ICT network equipment, similar to what the Commission dealt with in the USF context, but also video surveillance equipment and off-the-shelf camera equipment utilized by a range of small companies in addition to larger enterprises, as well as potential components authorized by the FCC that are widely deployed across the U.S.

[28] NPRM at ¶ 81.

The commercial nature and ubiquitous use of this video surveillance equipment makes it more difficult as a practical matter for the Commission to revoke authorizations and abruptly forbid equipment that had been sold in the U.S. marketplace for years. Therefore, if the FCC decides to require the removal of equipment that was authorized for sale at the time of purchase, despite the extreme burden to U.S. consumers and industry, there must be a fund to make affected parties whole similar to the mechanism authorized by Congress in the rip and replace proceeding.

The Commission should consider both the broad use of this equipment and the criticality of the function the equipment serves when considering whether revocation is justified in the first place, and then, whether there are any opportunities for U.S. companies to recover the cost of replacing covered equipment. In making this determination, the Commission should recognize the serious and unprecedented nature of any decision to revoke these authorizations, and that should weigh in favor of funding their replacement to underscore that this option will only be utilized in cases of national security. Any action on revocation must also acknowledge the cost to U.S. companies and consumers that have, acting in good faith upon existing authorizations, installed equipment from Covered Entities and should authorize funding to reimburse those companies.

When debating something as serious as revoking prior issued authorizations, the Commission owes it to U.S. consumers and the ICT industry to fully analyze the costs and benefits of the decision. If, after consultation with commenters in this docket, the Commission determines the benefit to U.S. security offered by revocation of equipment from Covered Entities outweighs the cost to the U.S. public, then it should only proceed if a mechanism exists to reimburse those affected by this move. To that end, the FCC should work with its partners in

industry and press Congress to authorize and appropriate funds to make affected parties whole should the extreme step of revocation be the best option to serve national security.

IV. THE FCC'S EQUIPMENT AUTHORIZATION RULES SHOULD NOT BE USED AS A METHOD FOR GOVERNMENT TO MANDATE SECURITY STANDARDS IN IOT DEVICES.

As the FCC considers its role in the critically important realm of ICT security, the Commission must rely on appropriate vehicles for regulating security. At a foundational level, the Commission's equipment authorization process was designed with technical, radio frequency ("RF") and interference matters in mind. If the FCC were to introduce security mandates into the existing authorization and certification process, it would require an extreme reconstitution of that process.

a. The FCC's Equipment Authorization Process Was Not Created with Security Matters in Mind.

In the NOI, the FCC contemplates expanding the existing equipment authorization regulations to include security elements for IoT devices.[29] The equipment authorization regime's legal foundation is the FCC's responsibility to prevent interference and reduce devices' susceptibility to interference from RF energy.[30] Specifically, Congress authorized the Commission to create equipment authorization regulations that may "make reasonable regulations," "consistent with the public interest, convenience, and necessity," of these goals.[31]

Any expansion of the equipment authorization process to cover cyber and security thresholds would go beyond this scope and authority of the FCC's powers for device approvals and equipment authorizations. Congress added Section 302 in 1968 to address interference caused by RF devices by enabling the FCC to regulate the manufacture, sale, and importation of

[29] NOI ¶ 101.
[30] 47 U.S.C. § 302a(a)
[31] *Id.*

such devices. The rare court cases examining the FCC's actions with respect to equipment authorization under Section 302 do not expressly reverse the FCC's decisions taken under Section 302 on substantive grounds. However, at least one court explained that although the FCC's grant in Section 302 is broad, it is the "same standard that governs the FCC's actions in a multitude of areas, and against which this court routinely judges the Commission's actions to determine whether they are arbitrary or capricious."[32]

To impose security requirements as part of the equipment authorization process, the FCC would have to articulate a legal nexus between securing devices and their potential to create interference. This is a thin reed on which to base an entirely new conceptual application of the equipment authorization process that is extended beyond the scope of Section 302. At a threshold level, botnets, data intercepts, and most all other current IoT cybersecurity incidents have not involved creating spectrum interference, and thus would fall largely out of the Congressional intent for the Commission's equipment authorization regulations.

b. Expanding the FCC's Equipment Authorization Powers to Include Cyber Issues Would Require an Extensive Rework of the Commission's Existing Process.

Should the FCC go down this path of expanding its equipment authorization process outside of its original scope to address security concerns, the Commission would be engaging in an extensive reworking of their existing scheme. It would also be imperative that the Commission works with Telecommunication Certification Bodies (TCBs) to ensure that an expansion of their work to include cybersecurity would be feasible.

The core of the FCC's equipment authorization regime is compliance testing: objective measurements by qualified laboratories of a representative sample device before a device is

[32] *Transp. Intelligence, Inc. v. FCC*, 336 F.3d 1058 at 1064 (D.C. Cir. 2003).

marketed or operated in the United States.[33] Approval then extends to all identical devices subsequently marketed to the sample tested.[34] Although there is some limited post-market surveillance and other requirements to present sample devices and records to the Commission,[35] the FCC's rules generally rely on one-time testing and forever marketing, unless the FCC changes its technical rules.[36] Further, to the extent that the equipment authorization process is used to advance goals unrelated to reducing harmful interference, such goals are accomplished via a demonstration of technical data (e.g., hearing aid compatibility) or simple check-the-box certifications (e.g., Anti-Drug Abuse Act).[37]

In contrast, effective cybersecurity is an ongoing process. As noted by the Commission, numerous trade groups and NIST have all provided guidance regarding ongoing or rapidly evolving practices that can *improve* cybersecurity.[38] These efforts demonstrate that effective cybersecurity requires far more than the one-time testing against static *technical* criteria or check-the-box certifications that the FCC effectively and efficiently leverages in its equipment authorization regime.

Further, assessing effective device cybersecurity requires different skill sets than those required to assess the technical rules underpinning the equipment authorization regime. Devices that connect to the network are generally authorized via the Commission's certification procedures because such devices often include transmitters to connect to networks and perform

[33] *See* 47 C.F.R. §§ 2.803, 2.805 (restricting the marketing and operation of RF devices, unless the device has an equipment authorization or qualifies for an exception).
[34] *See* 47 C.F.R. §§ 2.906, 2.907.
[35] *See, e.g.*, 47 C.F.R. § 2.962(g).
[36] *See Amendment of Parts 0, 1, 2, 15 and 18 of the Commission's Rules regarding Authorization of Radiofrequency Equipment*, First Report and Order, 32 FCC Rcd 8746 ¶ 26 (2017).
[37] NPRM ¶ 65 (discussing how the FCC uses the equipment authorization regime to implement certain statutory duties).
[38] NOI ¶ 99.

other functions.[39] Certifications are issued by Telecommunication Certification Bodies (TCBs) based on data measured by FCC-recognized accredited laboratories, among other factors.[40] TCBs must be FCC-recognized and accredited.[41] In the United States, NIST manages the TCB accreditation process and has recognized the American National Standards Institute and the American Association for Laboratory Accreditation to accredit TCBs located in the United States in accordance with ISO/IEC 17011, *Conformity assessment—General Requirements for Accreditation bodies accrediting conformity assessment bodies*.[42] The international standards guiding the accreditation of TCB-accreditation bodies, TCBs, and laboratories do not address the assessment of device cybersecurity.[43] Rather, the standards focus on being able to accurately measure, interpret, and record technical measurements such as those taken during electromagnetic, RF exposure, and hearing aid compatibility testing, and to assess bodies that interpret and perform the assessments.

Introducing device cybersecurity assessments in the certification process would require substantial changes to these international, consensus standards, which would likely take several years—if it could be accomplished at all. And even if the standards can eventually be modified, both the skills to meet the standard requirements as well as any test equipment then must trickle out to the accredited laboratories and TCBs (both in the U.S. and internationally) that test and

[39] Some other devices may exclusively rely on wired connections when connecting to networks and not include other intentional radiators. Such devices would very likely not be subject to certification. When those devices are subject to the FCC Supplier's Declaration of Conformity authorization regime, the labs testing the devices would encounter similar issues as accredited laboratories testing devices subject to certification such as learning unrelated new skills and purchasing new equipment.
[40] 47 C.F.R. § 2.962(f)(2).
[41] 47 C.F.R. § 2.962(c)(1).
[42] KDB Publication Number: 641163: TCB Program Roles and Responsibilities, https://apps.fcc.gov/oetcf/kdb/forms/FTSSearchResultPage.cfm?id=44683&switch=P.
[43] *See generally* 47 C.F.R. § 2.962; ISO/IEC 17065:2012 *Conformity assessment— Requirements for bodies certifying products, processes and services*; ISO/IEC 17025, *General requirements for the competence of testing and calibration laboratories*.

certify RF devices. Indeed, both lab and TCB personnel would very likely have to undertake extensive training in a new field and purchase new test equipment simply to be able to apply the modified standards. In the end, the equipment authorization regime that would emerge would hardly resemble the one that the FCC and industry have successfully and cooperatively applied for decades.

V. THE FCC SHOULD CONTINUE TO WORK WITH INDUSTRY AND EXISTING PUBLIC-PRIVATE PARTNERSHIPS TO SUPPORT INDUSTRY-DRIVEN STANDARDS AND CERTIFICATIONS FOCUSED ON ICT SECURITY.

When acting on cyber and supply chain issues, it is imperative for the FCC to not only remember the ongoing work from other agencies as part of a whole-of-government approach mentioned above, but also ongoing efforts from industry in the area. TIA has long said that while targeted action on ICT supply chain security is warranted in certain situations, we also believe the ICT industry itself is in the best position to lead when it comes to securing ICT devices and ICT supply chains.[44] We support the various industry-driven efforts to create standards and best practices supporting cyber and supply chain issues, as well as the numerous public-private partnerships that exist with the government focused on security issues.

As the NOI acknowledges, it is important for ICT manufacturers to build in security to their products.[45] Many industry groups have been focusing on this issue, for example, the C2 Consensus, which was led by the Consumer Technology Association with the help of 19 other associations, including TIA, and represents a consensus among ICT industry on baseline requirements for IoT devices.[46] Additionally, the Department of Commerce's National Institute

[44] *See, e.g.,* 2020 TIA Comments § I.
[45] NOI at ¶ 101.
[46] Council to Secure the Digital Economy, *The C2 Consensus on IoT Device Security Baseline Capabilities,* Sep. 2019 (*available at* https://securingdigitaleconomy.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf), supplemented in 2021 (*available at* https://csde.org/wp-content/uploads/2021/04/C2-Tech-Report_2021_final.pdf).

of Standards & Technology ("NIST) has played a leading role on IoT security, both through their publication *Foundational Cybersecurity Activities for IoT Manufacturers*,[47] as well as their coordination with the Federal Trade Commission on a consumer IoT Security Pilot required under the May 12 Executive Order on Improving the Nation's Cybersecurity.[48] These are just a few examples of many existing government and industry-driven programs to incentivize building in security measures to IoT devices, but demonstrate that the Commission is far from the first entity to examine IoT device security. As the Commission debates its role in the pressing cybersecurity matters facing the ICT community today, it is important that any action it takes works in harmony with these existing efforts.

TIA itself is working on an industry-led standard that is aimed at increasing the transparency for the ICT supply chain and encouraging ICT manufacturers to build in security as a subset of product quality.[49] Before the end of the year, TIA will release a comprehensive supply chain security process standard for the ICT industry that will address many of the security concerns contemplated in the NOI. The standard, named SCS9001, will be the first of its kind process-based standard based on existing gaps posed by security-related standards and best practices to create a comprehensive industry-driven standard to ensure the security of devices, equipment, and networks that comprise the ICT supply chain. TIA believes this standard and related third-party certification process will be useful for the FCC and other government agencies as they look to add more certainty to the security of IoT devices.

---

[47] National Institute of Standards & Technology, *Foundational Cybersecurity Activities for IoT Device Manufacturers* (*available at* https://csrc.nist.gov/publications/detail/nistir/8259/final).
[48] Executive Order on Improving the Nation's Cybersecurity (May 12, 2021) (*available at* https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/)
[49] https://tiaonline.org/what-we-do/technology-programs/supply-chain-security/scs-9001-ict-specific-standard-for-global-supply-chain-security/

Ultimately, TIA shares the concerns the FCC has when it comes to making sure IoT devices are secure, however, we believe that trying to regulate security through the equipment authorization process is not the correct approach, and we encourage the FCC to continue working with industry and partnerships that have already been developed. For instance, the Commission can work on its existing Communications Security, Reliability, and Interoperability Council ("CSRIC") Federal Advisory Committee that is already working on ICT Supply Chain Security to help advise the government on how it can promote the adoption and implementation of private sector certifications.[50] TIA's Senior Director of Government Affairs, Colin Andrews, was recently nominated to serve on CSRIC VIII, and we look forward to continuing the discussion of how the FCC can best promote industry-led efforts to secure the ICT supply chain while maintaining its critical role in promoting the deployment of secure and trusted ICT networks connecting the nation.

[50] Public Notice DA-430, *FCC Announces Intent to Re-Establish the Communications Security, Reliability, and Interoperability Council and Solicits Nominations for Membership* (Apr. 15, 2021) (*available at* https://docs.fcc.gov/public/attachments/DA-21-430A1.pdf).

CONCLUSION

TIA again thanks the Commission for leading the way on important national security issues facing the ICT sector. Our members are committed to building connected networks worldwide and promoting practices that ensure ICT networks are built by trusted vendors and manufacturers remains central to TIA's core mission as the trusted association for the connected world. TIA looks forward to continuing to work with the Commission as it works on the important issues raised by the NPRM and NOI.

By: */s/ Colin Andrews*

Colin Black Andrews
Senior Director, Government Affairs

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1310 N. Courthouse Road
Suite 800
Arlington, VA 22201
(703) 907-7700

September 20, 2021