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	)	

REPLY COMMENTS OF THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

October 18, 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	)	

REPLY COMMENTS OF THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

INTRODUCTION AND SUMMARY

The Telecommunications Industry Association ("TIA")[1] welcomes the opportunity to submit these reply comments in the above-captioned proceedings.[2] TIA believes in targeted government action on national security issues and, as the representative of global manufacturers and vendors of trusted ICT equipment and services that empower communications networks worldwide, believes that this proceeding is of the utmost importance for securing the ICT supply chain. TIA agrees with the majority of commenters in our support of the Commission's interest in ensuring that all equipment forming the foundation of U.S. ICT networks comes from trusted manufacturers and suppliers.

[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).

We believe the record shows industry support for a narrow, targeted action based on an extensive factual record to block Covered Entities from U.S. markets, but the Commission should ground this action in the Secure and Trusted Communications Networks Act ("SNA" or "Secure Networks Act") as opposed to Section 302 of the Communications Act.[3] The record further highlights the costs of retroactively revoking existing equipment authorizations from Covered Entities, and while this action may have some benefits, the FCC must be cautious to ensure that the substantial costs do not outweigh the benefits to the public. Finally, TIA shares commenters' skepticism about the questions raised by the NOI and potential Commission action that would include IoT security as a component of the existing equipment authorization process.

DISCUSSION

I. The Record Supports FCC Authority for Targeted Action Pursuant to Designations Under the Secure Networks Act, Not Section 302, to Exclude Covered Equipment from Future Equipment Authorization.

a. The Record Shows Broad Industry Support for the Commission's Objective in Securing the Nation's ICT Markets.

At its core, the issues raised by the NPRM are not new to the ICT industry – namely, what is the role of government in securing U.S. networks from equipment made by companies that pose a known and well-documented risk to national security. TIA is not new to these issues either – and as TIA has stated numerous times in various venues, we support narrowly tailored, targeted government actions to protect U.S. networks and consumers from ICT equipment that could pose national security risks. To that end, we agree with commenters who support the prospective removal of ICT equipment from entities that Congress, the Executive Branch,

[3] Communications Act, 47 U.S.C. § 302.

agencies with national security expertise, and the FCC itself have determined pose an unacceptable risk to national security.

TIA was not alone in supporting the Commission's objective in this proceeding – numerous commenters also filed in favor of the Commission's security goals underlying the NPRM. Based on the record, the ICT industry shares the concerns of the Commission with allowing ICT equipment that poses a national security concern to be sold in U.S. markets. However, TIA believes that the Commission must act in a narrowly-tailored fashion to address these issues while putting as small a burden as possible on trusted ICT vendors.[4]

While TIA supports the underlying goals and outcome of the rules proposed in the NPRM, we nevertheless urge the FCC to revise the proposed rules to achieve this goal in a more narrow, targeted way that provides regulatory certainty to the ICT industry without upheaving the existing FCC's equipment authorization process. Based on the record in this proceeding thus far, it seems likely that such a targeted, narrow approach would receive broader support from the ICT industry than the Commission's proposed path of utilizing the equipment authorization process and Section 302 of the Communications Act as an authority to bar equipment from Covered Entities.

b. The Record Demonstrates that the SNA, not Section 302, is the Appropriate Authority for Removing ICT Equipment from U.S. Markets Based on National Security Concerns.

Action to exclude ICT equipment from U.S. markets based on national security concerns should proceed according to the Secure Networks Act rather than Section 302 of the

[4] *See eg.* Comments from the Information Technology Industry Council at 1-2 ("ITI Comments"); Comments of NCTA – The Internet & Television Association at 4 ("NCTA Comments"); Comments of NTCA – The Rural Broadband Association at 1-2 ("NTCA Comments").

Communications Act and the FCC's equipment authorization process. TIA agrees with the majority of commenters who argue that the equipment authorization process is not the appropriate regulatory vehicle to exclude ICT equipment that poses a risk to national security.[5] Indeed, the majority of comments correctly observe that the equipment authorization process was created to tackle more technical issues such as RF exposure and interference issues.[6] As TIA explained in its initial comments, Section 302 of the Communications Act, the underlying statutory authority for the equipment authorization regime, addresses interference caused by RF devices, rather than the broader, national security concerns that the Commission seeks to address in this proceeding.[7] Other commenters broadly agree that Section 302 does not confer authority on the Commission to prohibit ICT equipment from U.S. networks.[8]

---

[5] *See, e.g.*, CTA Comments at 10 ("The Commission's Office of Engineering and Technology ('OET') professionals and the Telecommunications Certification Bodies ('TCBs') staff are experts at evaluating RF issues. But the proposals in the NPRM would expand the equipment authorization process beyond its traditional role, placing additional and novel security responsibilities on OET and TCBs, both at the review stage and an ongoing basis."); CTIA Comments at 15-20 (describing burdens on manufacturers, equipment authorization applicants, FCC staff, and others that may result from the NPRM's proposals to modify the equipment authorization process as proposed); Multi-Association Letter at 2 ("[T]he proposed changes to the equipment authorization rules will strain vital resources in the FCC's Office of Engineering and Technology ('OET')."); Tatel-Johnson Letter at 2 (noting that the equipment authorization process was "not based on, or authorized for, national security or cybersecurity functions" and is not "well-suited to being recast into performing such functions"); USTelecom Comments at 9-10 (observing that cybersecurity is an important aspect of network security as well as IoT/connected-device security, but many RF devices "are not and will never be 'connected' to a network, let alone communications networks and the public internet (*e.g.*, car key fobs, garage door openers, microwave ovens, pet trackers, home entertainment accessories)").

[6] *See, e.g.*, CTA Comments at 37 ("For more than 80 years, the FCC's equipment authorization inquiry has primarily been on narrow technical matters, such as limiting RF interference between devices and ensuring network compatibility."); ITI Comments at 14 (observing that "Section 302—the basis of the Commission's authority over electronic devices and equipment— makes no mention of cybersecurity, focusing exclusively on RF interference and related minimum performance standards"); Multi-Association Letter at 2 (noting that the proposals would "require gatekeeping a far larger scope of equipment for far different considerations than the FCC has traditionally examined"); Tatel-Johnson Letter at 2 ("The FCC's equipment authorization process is built upon the authority provided in Section 302 of the Communications Act to address harmful RF interference."); USTelecom Comments at 9 ("Section 302 of the Communications Act authorizes the Commission to make reasonable regulations governing the interference potential of devices that emit RF energy and to reduce home electronics' susceptibility to interference—issues that do not address the broad set of challenges regarding cybersecurity and IoT security risk management.").

[7] TIA Comments at 13.

[8] *See, e.g.*, CTA Comments at 39-40 (Section 302 limits the "Commission's consideration to 'interference potential' from 'radio frequency energy,' and does not give the agency free rein to consider broad security concerns beyond this technical inquiry"); NCTA Comments at 7 ("[T]he Commission should not rely on Section 302 as a standalone

That said, many commenters agree with TIA that the Commission has the authority to block equipment from Covered Entities under the SNA.[9] Specifically, the SNA is the "only existing statute that provides appropriate authority" for deeming covered equipment ineligible for the FCC's equipment authorization program."[10] We agree with CTA in their comments that "[t]he Commission's authority to prospectively prohibit any new Part 2 equipment authorizations for equipment on the covered list stems from the duties granted to the Commission under the SNA."[11] If the Commission adopts rules to prevent ICT equipment from entering U.S. markets in this proceeding based on national security concerns, the agency should rely on the SNA, rather than Section 302.

c. The Commission Has a Strong Factual and Policy Basis for Banning Covered Equipment.

As TIA outlined in our initial comments, the record on the Covered Entities at issue in this docket is extensive. In discussing the need for the FCC to act on national security concerns raised by ICT vendors that have been vetted through a whole of government approach, our initial comments detailed years of U.S. actions aimed at the five companies currently considered Covered Entities.[12] Unsurprisingly, numerous entities and subsidiaries of Covered Entities filed comments in response to the NPRM, arguing that the FCC's proposed rules lack authority and a tie to any factual basis. For instance, both Huawei and Dahua Technologies argued that banning

basis of authority for taking the action proposed in the NPRM, because there are substantial doubts as to whether that provision authorizes the contemplated action."); NTCA Comments at 2-3 (observing that the proposals to modify the equipment authorization to protect against cyber threats exceed the FCC's Section 302 authority).

[9] *See, e.g.*, Tatel-Johnson Letter at 2-3; NCTA Comments at 6 ("If the Commission opts to proceed prior to Congressional passage of the Secure Equipment Act, it should rely on the SNA, which in turn would ensure the efficacy of the covered list designations rendered under that Act.").

[10] Tatel-Johnson Letter at 3.

[11] NTCA Comments at 4.

[12] TIA Comments at II(b).

equipment based solely on the identity of its manufacturer would be "arbitrary and capricious."[13] Other Covered Entities argued that an action by the Commission to exclude their equipment lacked both legal authority and questioned the underlying factual basis of the proceeding.[14]

While we may agree with these entities that the Commission's authority to regulate national security concerns via Section 302 of the Communications Act is suspect, our initial comments made clear that TIA believes the SNA grants the FCC authority to exclude companies based on national security concerns, as discussed above.[15] However, one thing that these commenters seem to ignore is just how extensive of a record exists on the Covered Entities. The FCC's action in this proceeding to ban these ICT products from U.S. markets does not come as a single action – but is instead part of a whole-of-government approach to remove ICT equipment that poses security concerns from U.S. markets.

The truth of the matter is that Huawei, ZTE, Hikvision, Hytera, and Dahua have all been identified by numerous actions of Congress and the Executive Branch as security risks to the United States. For these five companies, this began with Congress labeling these companies as security concerns in the 2018 NDAA, and these concerns have only been reinforced in the years since. These companies are specifically labeled by Congress and the Executive as posing a threat to national security – and as we said in our initial comments, that threat applies whether we are dealing with entities that produce network equipment, or with companies that provide commercial-grade off-the-shelf equipment.

These commenters are incorrect to argue that the FCC is acting without any factual basis or authority in this docket when Congress has specifically tasked the Commission with keeping a

[13] Comments of Huawei Technologies Co., Ltd., Huawei Technologies USA, Inc. at 4; Comments of Dahuna Technology USA Inc, at 14-15.
[14] Comments of Hikvision USA, Inc. at 2, 7-27.
[15] TIA Comments at II(a).

list of suppliers whose equipment poses an "*unacceptable risk to the national security of the United States*."[16] As discussed above and in our initial comments, the authority in the SNA to keep this list is distinct from the requirement for the FCC to create a Rip and Replace fund. Because this authority exists independent from the singular Rip and Replace fund, it is a straightforward application of the FCC's authority under the SNA to take the logical step of removing equipment that has been shown to pose a risk to national security.

Congressional authority aside, the U.S. government has been developing a record on ICT national security risks posed by Covered Entities, ranging from efforts undertaken more recently by the Department of Commerce to actions taken by the Department of Defense after these entities were listed in the 2018 NDAA. The FCC itself has collected a record from ICT industry and U.S. consumers that clearly demonstrates that efforts targeting the Covered Entities are far from unexpected – there has been a whole-of-government approach aimed at removing their equipment for the better part of the last decade.

Any sort of argument that these rules would be arbitrary and capricious because they treat "similar" companies and products differently completely disregards this extensive record.[17] Technical specifications aside, when comparing two products the simple fact that one product is made by an entity that has been designated under U.S. law to pose a threat to national security is a sufficient basis to say that companies and products are not "similar."

Should the FCC proceed with adopting rules that exclude the five entities identified as threats to national security in the NDAA, SNA, executive orders, and the Commissions' own Covered List, there is more than enough record to stand on to show that this action is tied to legitimate security concern and would be in the public interest. Provided the Commission relies

[16] 47 U.S.C. § 1601 (*italics added for emphasis*).
[17] *See eg.* Hikvision Comments at 52.

on the authority discussed above, it would be hard to label the resulting action as disengaged from a factual basis or arbitrary and capricious.

II. The Record Identifies Expansive Issues that the FCC Must Consider in Determining Whether to Revoke Authorizations on a National Security Basis.

In our initial comments, TIA urged the Commission to consider the costs to the ICT industry and U.S. consumers before proceeding on any proposal to remove ICT equipment that has already been authorized by TCBs. On the record, ICT industry almost uniformly opposed the retroactive revocation of existing equipment authorizations. The Consumer Technology Association correctly points out that revocation would go beyond punishing Covered Entities and instead punish U.S. consumers who have done nothing wrong and purchased equipment relying on existing FCC authorizations.[18] CTIA similarly raises concerns with revocation harming consumers,[19] while ITI argues that the FCC lacks a legal basis to revoke existing authorizations.[20] In fact, in our review of the docket, we did not find a single comment from an ICT industry representative supporting the revocation of existing authorizations.

While TIA does not oppose the revocation of existing authorities *per se,* the response from industry on this issue underscores TIA's main concern with revocation in this proceeding – the cost of replacing this equipment given its broad, commercial, off-the-shelf nature. TIA does not argue that there is no public policy benefit in the actions contemplated by the NPRM. On the contrary, the national interest is served by ensuring equipment that includes known security vulnerabilities is not readily for sale in U.S. marketplaces, and revocation is an important tool that is potentially available to the government in serving that interest. However, any benefits to

[18] Comments of the Consumer Technology Association at 14-15.
[19] Comments of CTIA at 10-13.
[20] ITI Comments at 6.

national security must outweigh the costs to the ICT industry and U.S. consumers. Based on the record, it appears that the costs of the revocation proposed by the initial NPRM could outweigh any potential benefits. To that end, we continue to urge the Commission to extensively study the costs related to such a proposal to ensure that the benefit to the public does in fact outweigh the costs to U.S. consumers.

III. TIA Agrees with Commenters Skeptical of the NOI's Focus on the Equipment Authorization Process as a Means to Advance IoT Security.

As stated in our initial comments, TIA believes that the questions posed by the NOI regarding the possible expansion of the existing equipment authorization process to address IoT security concerns raise a broad spectrum of complicated legal and practical issues, and further Commission action in this area could have negative consequences for the entire ICT industry.[21] The vast majority of commenters who addressed the NOI echo these concerns and urge that the Commission proceeds with great caution in considering further action on the NOI, citing the potential disruption to emerging public-private approaches to IoT security that may otherwise result.[22]

TIA agrees with this consensus and again recommends that the Commission separate the issues raised in the NPRM from the NOI so that it can act promptly on the national security issues central to the NPRM while engaging more deliberately with industry on what the Commission's future role in IoT security should be.[23] Doing so will not stall broader efforts to enhance IoT security; on the contrary, NIST, DHS, and the FTC are all actively engaged on the subject and are well-positioned to drive further efforts, as various commenters describe.[24]

[21] *See* TIA Comments at 3-4.
[22] *See, e.g.*, USTelecom Comments at 12; 5G Americas Comments at 14.
[23] TIA Comments at 4.
[24] *See, e.g.*, CTIA Comments at 33-34; ITI Council Comments at 15.

Meanwhile, the Commission can complement these existing processes through steps such as directing the newly re-chartered CSRIC to develop recommendations to ensure IoT standards and certifications that will advance IoT security in 5G environments, as TIA and others have proposed.[25]

CONCLUSION

TIA thanks the Commission for working extensively with industry on these important national security issues, and we look forward to discussing these proposed rules and any further action under this docket with the Commission in the future.

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

October 18, 2021

[25] TIA Comments at 19; *see also, e.g.*, 5G Americas Comments at 2, 14; CTA Comments at 31-33; Tatel/Johnson Letter at 6.