

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

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

COMMENTS OF THE INFORMATION TECHNOLOGY INDUSTRY COUNCIL

The Information Technology Industry Council (ITI)¹ appreciates the opportunity to submit these comments to the U.S. Federal Communications Commission (FCC or Commission) in response to the Notice of Proposed Rulemaking and Notice of Inquiry in the above-captioned dockets seeking comment on proposed changes to the Commission’s equipment authorization rules.²

I. EXECUTIVE SUMMARY

ITI shares the Commission’s goal of securing domestic networks from national security threats, and, in fact, our association and members have spent considerable time and resources working to protect communications devices and networks. While the Commission

¹ ITI is the premier global advocate for technology, representing the world’s most innovative companies. Founded in 1916, ITI is an international trade association with a team of professionals on four continents. We promote public policies and industry standards that advance competition and innovation worldwide. Our diverse membership and expert staff provide policymakers the broadest perspective and thought leadership from technology, hardware, software, services, and related industries.

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*, ET Docket No. 21-232, EA Docket No. 21-233, Notice of Proposed Rulemaking and Notice of Inquiry, FCC 21-73 (June 17, 2021) (*Equipment NPRM/NOI*).

understandably is interested in contributing to U.S. government (USG) efforts to secure equipment and networks, taking steps to do so must appropriately address the Commission's authority and carefully consider whether factors pertaining to purported risks are significant enough to outweigh the substantial burdens likely to be associated with implementing the *Equipment NPRM/NOI*. ITI strongly agrees with the Commission that any actions taken with respect to the equipment authorization process should be taken "without delaying the authorization of innovative new equipment that benefits our lives."³

First, ITI recommends against the Commission proceeding with its proposal to revoke existing equipment authorizations. The lack of an adequate legal basis upon which to ground such a broad proposal should by itself urge caution on the part of the Commission and requires a pause. However, the implementation challenges of proceeding would create significant burdens and subject consumers, industry, and the Commission itself to the nearly insurmountable task of identifying all the specific equipment subject to revocation, sourcing and installing appropriate substitutes, and then auditing compliance. Importantly, the extreme hardships facing consumers and industry that would be expected to follow such a process have not been weighed against perceived benefits. The Commission has not articulated what increases in security it would expect to be achieved by implementing the revocation proposal, so it is unclear whether such a massive undertaking and the resulting disruptions would provide a measurable benefit in security.

Second, ITI opposes the Commission's overly broad proposal to bar the use of the Supplier Declaration of Conformity process based on the identity of the manufacturer, rather than adhering to the covered equipment criteria established by Congress. Further, the

³ *Equipment NPRM/NOI*, para. 46.

Commission improperly proposes to unilaterally expand its authority over Part 15 and other exempt devices by failing to limit its analysis to radio-frequency interference. ITI recommends against proceeding with either proposal due to clear statutory limits on the Commission's authority and the likely dampening of innovation that would follow. As with the equipment authorization revocation proposal, the Commission again fails to produce a cost-benefit analysis that might articulate a measurable expected increase in security.

Finally, while ITI agrees in general that securing Internet of Things (IoT) devices is an important policy objective, we recommend against proceeding with the Commission's proposal to use the equipment authorization program to address perceived risks or to engage in matters already under consideration by other expert agencies across the USG. Importantly, the Commission lacks statutory authority to engage in cybersecurity matters, while other federal entities have been directly tasked with doing so. Unilaterally engaging would be duplicative of other efforts and cause confusion within an already complex cybersecurity landscape. Moreover, in the absence of an expected increase in security, evidence of which the Commission does not provide, proceeding could create the potential for increased civil or regulatory liability that is ultimately unrelated to device security. The best way for the Commission to engage on this topic is to allow existing processes at other federal agencies to continue to proceed in conjunction with consumers and industry.

As a leading representative of innovators in all sectors of the technology industry, we can say with certainty that further innovation and competition in the market depend on an efficient, expertly staffed, and well-managed equipment authorization process. Certain Commission proposals could have the unintended effect of bogging down the authorization process or diverting the expertise of Commission staff in ways that would dampen innovation without a

corresponding increase in security. For these reasons, ITI urges to the Commission to exercise great caution in its approach to these matters.

II. REVOCATION OF EXISTING CERTIFICATIONS

While ITI shares the important goal of addressing unacceptable risks to national security in communications networks and equipment, we have significant concerns with the Commission's proposal to revoke existing equipment authorizations pursuant to section 2.939,⁴ which would, in effect, make the otherwise prospective ban on certain equipment authorizations retroactive. This approach should not be adopted by the Commission due to significant implementation concerns that vastly outweigh any perceived or potential increases in security. As detailed below, achieving the stated goal of securing domestic networks from national security threats requires the Commission to devote substantial time and resources toward (i) identifying specific equipment authorizations to be revoked, as well as (ii) ensuring that use of the relevant equipment throughout the U.S. is eliminated—both of which may result in extreme hardship to consumers. Importantly, ITI also has serious concerns with the lack of express authority for the Commission to revoke existing authorizations in the manner proposed, which strongly cautions against considering a blanket revocation of entire product portfolios for multiple companies, rather than carrying out the revocation analysis at the individual product level.

⁴ 47 CFR §2.939.

Lack of Legal Basis

As the Commission itself notes, the foundation of its equipment authorization process rests upon the statutory grant of authority to investigate the “interference potential of devices that emit radiofrequency (RF) energy and that can cause harmful interference to radio communications”⁵ and to make reasonable regulations to achieve this end.⁶ The Commission’s regulatory powers under section 2.939 to revoke existing authorizations are a reasonable outgrowth of the underlying statutory authority. If an applicant is found to have committed fraud by lying on an application or making relevant misrepresentations, or if the applicant has subsequently made changes to the equipment in a way that it no longer reflects what was originally certified, the revocation process exists as an appropriate remedy for removing components or equipment which have the potential to cause RF interference. Absent the threat of revocation, applicants would have no incentive to make truthful representations, and the Commission could not ensure that new and older communications equipment can coexist within the complex ecosystem made up of multi-layered communications networks.

The Commission’s proposal would expand the scope of the revocation process in ways not contemplated by the existing regulations or the underlying statute to achieve policy objectives that go beyond the well-established RF interference rules. While perhaps convenient from an administrative perspective, such an action would unmoor the revocation process from its firm reliance on technical data, objective performance characteristics, and the measurable harm that such products could create.

ITI opposes taking this approach. The Commission’s question of whether section 2.939(a)(4)’s reference to “conditions coming to the attention of the Commission” could be

⁵ *Equipment NPRM/NOI*, para. 23.

⁶ 47 U.S.C. §302a(a).

reasonably interpreted to mean, in effect, “newly adopted rules”⁷ must not be answered in the affirmative. As noted previously, section 302a of the statute is entirely centered around RF emissions and related minimum performance standards. Any “conditions” that may come to light after certification must have a bearing on the RF emissions analysis or relate to case-specific facts that would have been disqualifying *for a particular applicant* in the first instance.⁸ Otherwise, section 2.939(a)(4) would, in effect, grant the Commission virtually unlimited authority to rewrite the rules of the process arbitrarily and at any time, without regard for whether the new conditions are at all related to the functionality of equipment or its potential to cause RF interference.

Carrying out revocation in the manner proposed by the Commission would likely diminish the value of an FCC equipment authorization by calling into question whether *any* authorization could be revoked at any time, for reasons other than those currently established in law, such as technical failures or fraud in the application process. This milieu hanging over the communications equipment sector would reduce incentives to innovate and ultimately could prove costly to consumers who may no longer have access to new or improved equipment and services that provide needed access to the benefits of the digital economy. Such an outcome would directly conflict with the FCC’s efforts to make communications technologies available to all Americans and to close the digital divide.

Further, the Commission’s tentative conclusion that it would be appropriate to stretch the definition of “technical standards”⁹ to provide a basis for enforcing retroactive revocations¹⁰ is equally as problematic as broadening the meaning of “conditions,” if not more so. ITI opposes

⁷ *Equipment NPRM/NOI*, para. 85.

⁸ *See id.*, para. 85, n.227.

⁹ *Equipment NPRM/NOI*, para. 86.

¹⁰ 47 CFR § 2.939(c).

adoption of this approach as well. As noted, the plain language of the statute speaks to RF emissions and related performance standards exclusively. There is no mention of unilateral revocations absent technical analysis. Indeed, Subpart J of the regulation begins in section 2.901 by spelling out that RF “equipment and parts or components thereof” are subject to specific “technical standards” depending on the individual type of equipment to be certified and which rule part governs “the service wherein the equipment is to be operated.”¹¹ It follows that an entity seeking an equipment authorization would expect to review device-specific rules that describe in detail the functional parameters within which the equipment may operate, including spectrum frequencies, out-of-band emissions, etc.

In fact, section 2.1033(b)(6) describes a series of *measurements* that must be made as part of the initial application.¹² Throughout Subpart J the Commission describes with granularity the types of quantitative data that must be included with applications for various types of equipment and components. It would be inappropriate to shoehorn into the meaning of the term “technical standards” in section 9.939(c) an attestation requirement stating that the applicants’ equipment is not included on the Covered List, however worthy the objective may be. This would clearly be a policy determination, and not a technical requirement. Read in the context of the whole regulation and pursuant to the underlying statute, broadening the meaning of “technical” beyond frequency use, out-of-band emissions limits, power levels, or other widely accepted, measurable characteristics, would ultimately render the term “technical” either all-encompassing, or perhaps utterly meaningless.

¹¹ 47 CFR § 2.901(a).

¹² *Id.* § 2.1033(b)(6).

Implementation Challenges Create Significant Burdens

While ITI maintains that the Commission lacks the authority to revoke existing certifications for “covered” equipment out of hand, if the Commission were to move forward with a retroactive ban there are myriad practical challenges involved with doing so that the Commission should carefully consider before proceeding. Any approach is likely to create substantial industry and consumer confusion, burden, and expense.

In its proposal, the Commission rightfully asks whether there is an existing process for identifying particular authorizations to be revoked.¹³ The problem of developing an appropriate methodology for sifting through hundreds of thousands, if not millions, of existing authorizations is enormous, and would be both unprecedented and virtually insurmountable based on ITI’s understanding of the impacted industries. Most certified equipment that has been approved for use has already entered the stream of commerce and is in the hands of end users, which could range from individuals to small businesses or to large enterprises and even global entities. The operational reality, which complicates the administrative problems substantially, is that most, if not all, covered equipment is not sold directly to consumers in the first place—often being sold from manufacturers to distributors, to resellers, to installers, and then to end user consumers, which range from large businesses to individuals. Thus, it is unclear which entity or consumers would bear responsibility for identifying covered equipment and ensuring compliance with new rules as proposed.

Another example is where a manufacturer incorporates equipment components into a larger system where those components are not labeled with the name of the component manufacturer. There could also be distributors, value added resellers, installers, and service

¹³ *Equipment NPRM/NOI*, para. 88.

providers that handle the covered equipment without the end users even knowing that such equipment is incorporated into or is being used for their benefit. Not only would each system need to be located and then analyzed for compliance, but each individual component would need to be analyzed as well. Yet, for equipment that has left the hands of the manufacturer, the difficulty of trying to identify and locate equipment that has changed hands multiple times, along with the confusion of all parties involved in the supply chain, is one of enormous proportions.

Even if the broad range of potentially implicated equipment could be identified and located, significant questions would remain as to which parties would bear the liability for sourcing replacement components and equipment and who would be responsible for doing the work, given the various touches each piece of equipment receives between the manufacturer and end user. In the case of larger systems that may be impacted due to their inclusion of certain components, re-engineering would likely be required, along with reapplication for authorization, which includes extensive testing and validation. All these circumstances are further complicated by the fact that certain businesses in the supply chain may bear a disproportionate share of the financial burden. Installers and service professionals will be approached directly by end customers, and resellers and distributors may point to manufacturers—stating that they relied on manufacturers to obtain the authorizations. The key question is, would end users or manufacturers be liable for sourcing replacement equipment, or service providers such as installers, or the end users themselves? And, would there be federal funding to help to cover these costs regardless of which entity is determined to be liable for the replacement?

Further, as ITI has noted previously, manufacturers are already facing significant challenges in meeting demand for new communications equipment even with the semiconductor

industry operating at historically high capacity.¹⁴ Equipment manufacturers would certainly face further pressures where there are not existing 1:1 replacement offerings or suitable alternatives already available in the market to replace equipment for which the certifications may be revoked. Where an entire industry would be required to simultaneously remove and replace the covered equipment immediately, it would be extremely challenging, if not impossible, to find cost-effective offerings that could be obtained in a timely manner to satisfy new product sales and replacement needs going forward.

Finally, these concerns relate to industry and the private sector, but there are also question as to whether the FCC would be charged with enforcing this process and auditing compliance. Doing so would take up substantial resources and almost certainly bog down the Commission's work on new certifications and other important agency functions, which the Commission has agreed are a high priority.¹⁵ If the Commission were to move forward with the revocation proposal, it is critical that an adequate transition period be established which takes into account the many complex variables that relate to identifying, sourcing, and replacing the equipment, along with the Commission's own capacity to manage such a process. At a minimum, this would mean considering both pandemic market conditions and related delays, including increased demand for connected devices, while addressing the additional supply chain pressures that would occur should all covered equipment authorizations be revoked.

¹⁴ See Comments of the Information Technology Industry Council, *WTB Seeks Comment on Impact of Global Semiconductor Shortage*, WT Docket No. 21-195 (filed June 10, 2021).

¹⁵ *Equipment NPRM/NOI*, para. 46.

III. SUPPLIER DECLARATION OF CONFORMITY AND EXEMPT DEVICES

Barring the use of the Supplier Declaration of Conformity (SDoC) process based on the identity of an “entity” rather than the nature of the “covered” equipment is overly broad and ignores existing law and regulations regarding the specific types of equipment that the USG has determined may pose a threat to national security. The Covered List relates to specific types of equipment or services that have been assessed by certain federal authorities to pose specific potential threats, and the statute spells out a two-part test that must be met before the Commission may carry out its required updating of the list.¹⁶ First, the equipment or service must be produced or provided by an entity that has been determined to pose “an unacceptable risk to the national security of the United States,”¹⁷ and it must possess certain technical capabilities,¹⁸ which the Commission has interpreted to mean “can possibly perform these functions.”¹⁹

However, in the current proposal, the Commission seeks to prohibit the use of the SDoC process based exclusively on the identity of the entity, rather than relying on the full potential threat analysis to be carried out as Congress intended. ITI opposes such a broad approach, which would dramatically expand the scope of the FCC’s role in the process. If any changes are to be made to the SDoC process, the rules should be grounded in clear legal and regulatory bases that incorporate proper application of the statutory covered equipment criteria. The expansive reach of the Commission’s SDoC proposal could capture a range of equipment not contemplated by Congress or the other expert agencies tasked with determining which equipment should be included on the Covered List.

¹⁶ 47 U.S.C. § 1601(b).

¹⁷ *Id.* § 1601(b)(1).

¹⁸ *Id.* § 1601(b)(2).

¹⁹ *Equipment NPRM/NOI*, para. 17.

Further, the FCC should not proceed with unilaterally expanding its authority over Part 15 and other exempt devices and components beyond existing statutory authority related to RF interference complaints.²⁰ Requiring attestations or a central registry for exempt devices would be a staggeringly overbroad approach, create enormous administrative burdens for industry and the Commission, and quickly dampen innovation in the market. One of the greatest benefits of having exempt classes of equipment is that they operate in an appropriately risk-based environment. With a relatively low risk profile due to relatively low emissions, there is virtually no limit on the creative potential for developers to build devices and components to be quickly deployed if they adhere to minimum interference standards. The complaint process allows violators to be reported and dealt with accordingly.

By their nature, the exempt class of devices and unintentional radiators exists precisely because of the low interference potential, and as such, the idea that these devices or components would as a class pose a potential national security risk is questionable on its face. However, to the extent exempt devices do create potential national security risks, one would expect those specific devices to meet the covered equipment criteria, obviating the need for such a broad expansion of the Commission's reach. Notably, the FCC argues that a cost-benefit analysis is unnecessary due to the exigency of addressing national security concerns,²¹ but in dispensing with the analysis, the Commission fails to consider the disproportionate burdens that the proposal would saddle on consumers, manufacturers, resellers, and installers of equipment.

Overnight, equipment users in all these categories would suddenly be swept into the FCC's purview. And they would be subject to the extreme burden of being required to source replacement equipment with few alternatives. As noted, replacements would be costly, difficult

²⁰ *Equipment NPRM/NOI*, para. 75.

²¹ *Id.*, para. 79.

to source, and in many cases, would not actually be 1:1 replacements. To the extent the agency seeks to expand its reach beyond statutorily mandated covered equipment, it is obligated to provide a cost-benefit analysis that accounts for actual risks and actual costs. Here, the Commission has not even attempted to state whether or how such a broad effort would provide a measurable increase in public safety or improvements to national security. ITI recommends that the Commission reconsider its exempt devices proposal to avoid seeing a national security threat in every unintentional radiator.

IV. NOTICE OF INQUIRY

While ITI agrees that securing Internet of Things (IoT) devices is an important policy objective, we have significant concerns regarding expanding the Commission's equipment authorization program to address cybersecurity risks in IoT devices. As noted in the *Equipment NPRM/NOI*, numerous initiatives exist across the USG to encourage equipment manufacturers to improve the security of IoT devices. ITI supports these initiatives, which take a collaborative approach to defining IoT cybersecurity standards and incorporate both industry input and government expertise. The FCC, however, lacks both expertise and clear legal authority to regulate IoT device cybersecurity, through the equipment authorization program or otherwise. Any such initiative would represent a significant expansion of the Commission's existing equipment authorization program and a deviation from its core public policy objective of minimizing RF interference. The FCC's role is not appropriate as a potential enforcer of otherwise voluntary or collaborative standards, and therefore, ITI opposes measures where the Commission seeks to take steps to insert itself into the regulation of IoT device security or related product requirements, whether in substance or through enforcement.

Most importantly, the Commission lacks statutory authority to regulate IoT security. 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.²² Although the Secure and Trusted Networks Act²³ provides the Commission with specific, limited authority to address potential national security risks facing U.S. communications networks posed by certain equipment, nowhere does the statute grant the Commission any authority to establish cybersecurity standards for IoT devices or require applicants seeking equipment authorizations to certify the security of their devices or otherwise disclose the voluntary processes they may follow to improve the security of IoT devices.²⁴ Indeed, the Commission does not make a compelling case for possessing the requisite authority but suggests, instead, that due to the ongoing USG efforts to address cybersecurity that the FCC should consider becoming involved as well.

The potential benefits of incorporating IoT security certifications (voluntary or otherwise) are also unclear. Manufacturers are currently free to certify their IoT devices to existing cybersecurity standards that both communicate their cybersecurity commitments to customers and provide a foundation for auditable security.²⁵ The operational reality is that cybersecurity-related certifications or disclosures would not substantively enhance product security but would only serve to create the potential for increased civil or regulatory liability unrelated to the improvement of device security. Therefore, the Commission should avoid using the equipment

²² 47 U.S.C. § 302a.

²³ *Id.* § 1601 *et seq.*

²⁴ *See id.* § 1603(d)(4)(B)(ii), which does require applicants seeking reimbursement under the Secure and Trusted Networks Act for replacement equipment to certify that they “will consult and consider the standards, guidelines, and best practices set forth in the [NIST] cybersecurity framework.” Notably, this provision does not grant additional authority to the Commission itself to impose mandates on the applicants or otherwise regulate their cybersecurity practices.

²⁵ *See, e.g.,* UL, *IoT Security Rating Helps Demonstrate Product Security to the Marketplace* (May 11, 2020), <https://www.ul.com/news/uls-iot-security-rating-helps-demonstrate-product-security-marketplace>.

authorization process overly broadly. In addition to the FCC lacking substantive authority, as a practical matter, there are numerous existing and ongoing efforts by expert agencies that are better positioned to address IoT security and have the existing and necessary authority to do so. In the interest of regulatory comity, the Commission should approach the topic with great caution to avoid duplicating numerous ongoing USG efforts and adding yet another layer to an already confusing and crowded cybersecurity landscape.

The best way for the Commission to engage on this topic is to allow expert agencies such as the National Institute of Standards and Technology (NIST) and the Federal Trade Commission (FTC) to continue working across the USG, in conjunction with consumers and industry, to provide helpful guidance and processes for manufacturers. NIST has conducted extensive work on IoT security, and pursuant to the Cybersecurity Executive Order 14028, it has already been tasked with leading the Consumer IoT cybersecurity labeling program. While ITI has worked extensively with NIST and the FTC on this and many other efforts, neither ITI nor our members have identified gaps in the process that could be filled by the FCC. In particular, the Office of Engineering and Technology (OET) may lack the institutional background and requisite staffing levels needed to cover cybersecurity issues and to contribute substantively to the work already underway at other agencies such as NIST and the FTC.

In general, ITI has strongly supported risk-based approaches to IoT security²⁶ and has found it helpful to leverage globally accepted supply chain risk management standards like ISO 28000 or ISO 27701, which allow vendors to demonstrate their compliance based on consistent standards and evaluation. Additionally, industry has been actively engaged in developing

²⁶ See ITI, *IoT Security Policy Principles*, <https://www.itic.org/dotAsset/d9c7be68-d2d4-42de-aaca-e91fc526b717.pdf> (last visited Sept. 20, 2021); see also Council to Secure the Digital Economy, *IoT Security Policy Principles*, <https://www.ustelecom.org/wp-content/uploads/2021/04/2021-CSDE-Policy-Principles-FINAL.pdf> (last visited Sept. 20, 2021).

voluntary standards and specifications building on NISTIR 8259, 8259A series for certain IoT Sectors (e.g., CTA 2088), and ITI and the global technical standard expert community are working to develop standards such as ISO/IEC 27402 IoT security and privacy (in draft). Similarly, on the global stage, ITI has supported participation in industry-led bodies with transparent, rules-based processes in place.²⁷ These are just some of the many efforts already underway elsewhere.

In sum, ITI believes that the FCC lacks legal authority to expand the equipment authorization process to address IoT cybersecurity and that IoT cybersecurity standards are best developed through existing collaborations between industry, standards development organizations, and expert agencies such as NIST and the FTC.

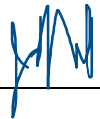
V. CONCLUSION

While ITI shares the stated goals of the Commission to increase supply chain security and the cybersecurity of certain connected devices, on balance we must oppose the Commission's proposals to revoke existing equipment authorizations, to bar the use of the SDoC process in certain cases, to expand agency authority over exempt devices, and to engage unilaterally in USG processes designed to improve the cybersecurity of IoT devices. In each case, the Commission lacks a clear statutory grant of authority, the practical challenges of proceeding would create significant burdens, and in none of these matters has the Commission articulated an expected benefit of increased security. As the FCC considers taking steps to secure U.S. equipment and networks, we urge it to do so in a way that appropriately addresses its authority

²⁷ See ITI Comments in Response to NTIA request for public comment on Implementation Plan for National Strategy to Secure 5G; RIN #0660-XC04; Docket No. 200521-0144 (June 25, 2020) <https://www.ntia.doc.gov/files/ntia/publications/iti-council-0625220.pdf>.

and carefully considers whether factors pertaining to purported risks are significant enough to outweigh the substantial burdens likely associated with implementing the proposed rules.

Respectfully submitted,

By:  _____

Joel Miller
Senior Director of Policy
Information Technology Industry Council
700 K St NW
Suite 600
Washington, D.C. 20001

September 20, 2021