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 CTIA

Thomas C. Power
Senior Vice President and General Counsel

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

John A. Marinho
Vice President, Technology and Cybersecurity

Melanie K. Tiano
Assistant Vice President, Cybersecurity and Privacy

CTIA
1400 16th Street NW, Suite 600
Washington, D.C. 20036
202-736-3200

September 20, 2021
TABLE OF CONTENTS

I. INTRODUCTION AND SUMMARY ................................................................. 2

II. THE INTEGRITY AND COMPETITIVENESS OF U.S. COMMUNICATIONS NETWORKS AND TECHNOLOGY ARE CRITICAL .............................................................. 3
   A. The Wireless Industry Safeguards U.S. Networks, Including From Foreign Threats ...................... 3
   B. The Commission Should Support a Unified, Risk-Based Approach to ICT and Supply Chain Security ........................................................................................................ 6
   C. A Well-Functioning Equipment Authorization Program Is Essential to Technological Innovation and American Competitiveness ......................................................... 8

III. IN RESOLVING THE NPRM, THE FCC SHOULD MINIMIZE IMPLEMENTATION CHALLENGES, REGULATORY BURDENS, AND CONSUMER HARM ........................................... 9
   A. Revoking Existing Equipment Authorizations Would Impact the Entire ICT Economy, Create Serious Complications, and Harm Consumers ......................................................... 9
   B. The Proposed Bidding Certification Should Be More Tailored ....................................................... 13
   C. The NPRM Raises Several Compliance Challenges for Participants in and Beneficiaries of the Equipment Authorization Regime .................................................................................. 15
   D. It is Vital that The Commission Account for the Costs and Benefits of Changes to Its Equipment Authorization Regime ................................................................................................ 17
   E. Legal Issues in the NPRM May Make Alternative Approaches Preferable ................................ 20

IV. WITH RESPECT TO THE NOI, THE COMMISSION SHOULD SUPPORT UNIFIED IOT SECURITY WORK IN PARTNERSHIP WITH THE PRIVATE SECTOR, AND REFRAIN FROM PURSUING DISRUPTIVE REGULATIONS ................................................................. 23
   A. The Wireless Industry Is Securing the IoT Ecosystem to Enable a 21st Century Connected Life .... 23
   B. CTIA’s Members Are Working with Federal Stakeholders on IoT Security ........................................ 25
   C. IoT Security Is Best Addressed Through Flexible, Voluntary, and Risk-Based Solutions ......... 28
      1. There Is No One-Size-Fits-All Solution to Device Security ....................................................... 28
      2. Cybersecurity Is Ill-suited for Static, Regulatory Approaches .................................................... 29
      3. Creating and Superintending a New Equipment Cybersecurity Regime Would Require Substantial New Resources and Capabilities ................................................................. 32
   D. The FCC Can Help Supplement NIST’s IoT Work and Support Advancements in Industry-Led Efforts ............................................................................................................ 33
   E. The Communications Act Does Not Authorize the FCC to Pursue the Cybersecurity Proposals Set Forth in the NOI ................................................................................................ 35

V. CONCLUSION .................................................................................................. 39
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 CTIA

CTIA\(^1\) submits these comments on the Federal Communications Commission’s (“FCC” or “Commission”) Notice of Proposed Rulemaking and Notice of Inquiry in the above-referenced proceedings, in which the Commission seeks input on proposals aimed at mitigating national security threats by making changes to the Commission’s equipment authorization and competitive bidding regimes, and asks about how to promote security in connected devices.\(^2\)

While CTIA supports the Commission’s important objectives in these proceedings, CTIA urges the Commission to ensure that any changes to FCC rules appropriately account for implementation complexities, minimize regulatory burdens that could stifle innovation and harm

\(^1\) CTIA® (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st-century connected life. The association’s members include wireless carriers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry’s voluntary best practices, hosts educational events that promote the wireless industry, and co-produces the industry’s leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.


1
consumers. The Commission should promote a risk-based, unified governmental approach to national security and cybersecurity issues.

I. INTRODUCTION AND SUMMARY.

CTIA and its members share the Commission’s goal of protecting wireless networks and equipment from national security and cybersecurity threats. Security is essential to a robust fifth generation (“5G”) wireless economy and a thriving Internet of Things (“IoT”) industry. The wireless industry is leading on information and communications technology (“ICT”) security, collaborating with government and other stakeholders to deploy risk-based solutions to enhance the security of U.S. communications networks.

The speed and predictability of the Commission’s equipment authorization regime have propelled American innovation for decades, allowing industry to bring new technologies to market quickly. With the rise of 5G and IoT, millions of new devices will be subject to the equipment authorization regime over the next few years. The Commission should ensure that any changes to the framework do not undermine the efficacy of the equipment authorization process or hinder innovation.

Some of the NPRM’s proposals could have significant unintended consequences. In particular, the NPRM’s proposal to revoke equipment authorizations will be difficult to implement, harm American consumers, and weaken supply chains. The proposal to adopt an additional competitive bidding certification may create compliance challenges and frustrate efforts to ensure that spectrum is put to its highest use. The Commission should revisit these proposals to consider more tailored approaches. More broadly, the Commission should address compliance challenges raised by the NPRM and must account for the costs and benefits of proposed changes, including burdens that may be passed on to consumers.
The NOI extends far beyond national security concerns, contemplating sweeping regulatory oversight of the cybersecurity features of the connected devices and systems that will drive the 5G future and beyond. The wireless industry has been active on this for years, working with federal stakeholders on IoT security. As these efforts show, cybersecurity is best addressed through public-private partnerships and flexible, risk-based solutions, not prescriptive mandates. Rather than duplicating the ongoing work of its federal partners, the Commission should support industry-led efforts, promote the National Institute of Standards and Technology's (“NIST”) leadership on voluntary and flexible guidance for IoT security, and look to the Communications Security, Reliability and Interoperability Council (“CSRIC”) for input.

II. THE INTEGRITY AND COMPETITIVENESS OF U.S. COMMUNICATIONS NETWORKS AND TECHNOLOGY ARE CRITICAL.

As the Commission evaluates proposed changes to the equipment authorization and competitive bidding regimes to promote national security, three principles should guide its approach: (i) federal policies should be cognizant of the ongoing work of the wireless industry to safeguard U.S. networks; (ii) ICT supply chain security requires a unified, risk-based approach; and (iii) a well-functioning equipment authorization regime is essential to the provision of communications services as well as American innovation and competitiveness.


CTIA's members know the importance of national security to the communications industry. As the Commission has recognized, "in today’s increasingly connected world, safeguarding the security and integrity of America’s communications infrastructure has never
been more important.”3 Security is key to unlocking the tremendous consumer benefits that will flow from advances in 5G and IoT. That is why the entire wireless ecosystem—network operators, device manufacturers, operating system developers, application service providers, and others—works together to develop security features to protect networks and consumers.

The wireless industry prioritizes security across networks, devices, and supply chains. Collaborating across government and industry sectors, CTIA’s members have been proactive, building security into wireless networks from the ground up, designing devices with robust security features, and engaging on supply chain efforts.

**Network Security.** The wireless industry prioritizes security, as shown in the end-to-end security architecture of 4G LTE and 5G, which use capabilities such as cryptographic protection and mutual authentication to ensure a secure environment.4 And while security has always been a priority, industry has enhanced security with each generation of wireless service.5 5G is no different, as industry standards for 5G have been “designed and specified . . . to include many new cybersecurity features and capabilities that improve upon 4G LTE.”6

---


5 See id. (“When compared to previous cellular networks, the security capabilities provided by LTE are markedly more robust.”).

Device Security. On the device side, strengthening security “cultivates trust and fosters an environment that enables innovation on a global scale.” Industry works hard to secure the IoT ecosystem and protect customers. The industry has also collaborated with expert agencies like NIST to define baseline voluntary approaches to foundational IoT security and advance industry and international standardization. The wireless industry has been a leader on IoT, establishing a first-of-its-kind IoT Cybersecurity Device Certification Program for cellular-connected devices run by CTIA and contributing to the Council to Secure the Digital Economy’s C2 Consensus on IoT Device Security Baseline Capabilities, among other work.

Supply Chain Security. The wireless industry has been proactive on supply chain security by implementing risk management policies and imposing security requirements on suppliers and contractors. The industry also collaborates with the government. For example, CTIA has been active in the Commission’s recent Universal Service Fund (“USF”) supply chain proceeding and in the CSRIC. The industry works with the Department of Homeland Security

---


10 See, e.g., Comments of CTIA, WC Docket No. 18-89, at 5-6 (Feb. 3, 2020) (describing significant efforts by AT&T, Verizon, and T-Mobile to enforce security policies and standards that safeguard supply chain security) (“CTIA Supply Chain FNPRM Comments”).
supports risk management by the Cybersecurity & Infrastructure Security Agency ("CISA"), and engages with the Department of Commerce ("Commerce") and the National Telecommunications and Information Administration ("NTIA") on supply chain, including the Communications Supply Chain Risk Information Partnership ("C-SCRIP"). Finally, CTIA and its members collaborate with NIST on communications and IoT supply chain and cybersecurity, including the Cybersecurity Framework’s expansion to “Cyber Supply Chain Risk Management,” and the development of Cybersecurity Supply Chain Risk Management ("C-SCRM") tools.


The global ICT supply chain and IoT raise challenges due to their diverse and evolving nature. This rapidly changing landscape requires a risk-based, unified federal approach, led by agencies with security expertise. A coordinated, risk-based approach must encompass the entire IoT ecosystem and focus on segments that present the greatest risks. For example, unmanaged devices connected to Wi-Fi or Bluetooth present different risks than managed devices. A


unified, federal approach should identify and account for different risk factors to maximize security.

As the sector-specific agency for communications and information technology, DHS is positioned to drive action on ICT and supply chain security, with Commerce playing a key role.\textsuperscript{16} DHS has a proven history of successful collaborations with the private sector and has the tools and resources to lead on ICT security, with access to intelligence agencies and information critical to making timely, risk-based determinations.

The Commission should proceed cautiously as it considers policies that overlap with other government activity. DHS, Commerce, and other federal agencies have significant expertise and are actively engaged in ICT and IoT security. Notably, NIST and the Office of Management and Budget ("OMB") serve key roles in defining cybersecurity frameworks. In particular for IoT, President Biden’s Executive Order on Improving the Nation’s Cybersecurity addressed IoT in a way that recognizes its complexities, directing NIST to “initiate pilot programs informed by existing consumer product labeling programs to educate the public on the security capabilities of [IoT] devices” and to work with the Federal Trade Commission ("FTC") to “identify IoT cybersecurity criteria for a consumer labeling program.”\textsuperscript{17} NIST has been collaborating with industry on defining a voluntary consensus for IoT security, and has traditionally coordinated industry voluntary cybersecurity testing within the federal government.

In light of these ongoing activities, the Commission should exercise caution about its role in cybersecurity and national security. As the Fifth Circuit recently observed, the FCC’s role in

\textsuperscript{16} See CTIA Supply Chain FNPRM Comments at 9-10.

\textsuperscript{17} Executive Order 14028, Improving the Nation’s Cybersecurity, 86 Fed. Reg. 26633, § 4(s)-(t) (May 12, 2021).
national security “for decades” has consisted of “limited, communications-focused judgment
informed by expert agencies and deferential to their views.”

Given this, the Commission should promote a risk-based, unified federal security response, led by DHS.

C. A Well-Functioning Equipment Authorization Program Is Essential to Technological Innovation and American Competitiveness.

The FCC’s equipment authorization regime has been a cornerstone of American innovation and technological advancement since its inception. With the Office of Engineering & Technology’s (“OET”) guidance, Telecommunications Certification Bodies (“TCBs”) have developed expertise at analyzing and addressing RF issues to keep the equipment authorization program running smoothly. A diverse array of entities rely on a timely authorization process to bring their devices to market. Innovators, manufacturers, and retailers often make product design and supply chain decisions based upon the FCC’s equipment authorization requirements.

As the Commission notes, a well-functioning equipment authorization process “further[s] the communication sector’s ability to drive innovation that will advance America’s global competitiveness and promote economic growth.” To this end, companies rely on being able to develop and obtain FCC approval for innovative devices in a timely manner. As the pace of innovation has increased in the Internet age, the Commission has, from time to time, streamlined and modernized its equipment authorization rules to ensure that the regime does not stifle

---

18 Huawei Techs. USA, Inc. v. FCC, 2 F.4th 421, 443 (5th Cir. 2021) (emphasis added).

19 See 47 C.F.R. § 2.962(c) (outlining expertise requirements for designation as a TCB, including “the technical expertise and capability to test the equipment it will certify,” and accreditation).

innovation or slow technological progress.\textsuperscript{21} With the deployment of 5G and the explosive growth of IoT, the regime will be put to the test with myriad new devices.\textsuperscript{22}

To ensure that the United States remains a leader in emerging communications technologies, the Commission’s equipment authorization process must be as efficient and streamlined as possible. But the NPRM proposes to add additional requirements that reach beyond identified national security threat actors. The Commission should reconsider the NPRM’s approach to ensure that any new rules are narrowly tailored to known threats and are still able to promote the equipment authorization regime’s longstanding goals.

III. IN RESOLVING THE NPRM, THE FCC SHOULD MINIMIZE IMPLEMENTATION CHALLENGES, REGULATORY BURDENS, AND CONSUMER HARM.

A. Revoking Existing Equipment Authorizations Would Impact the Entire ICT Economy, Create Serious Complications, and Harm Consumers.

The NPRM asks whether the Commission should “revoke any existing equipment authorizations of … ‘covered’ equipment pursuant to [the FCC’s] section 2.939 revocation rules.”\textsuperscript{23} Revoking existing equipment authorizations for covered equipment would present serious challenges and has the potential to harm to American consumers.\textsuperscript{24}

\textsuperscript{21} NPRM ¶ 24-26.

\textsuperscript{22} As CTA and others have advised, 5G may require even more streamlining of the equipment authorization regime as innovators race to meet consumer demand. \textit{See Comments of CTA, ET Docket No. 20-382, RM-11857, at 2 (Feb. 11, 2021) (“Innovative companies racing to develop and deploy products and services for the 5G economy need greater flexibility to market and pre-sell devices so that they can meet customers’ needs and expectations.”)}.

\textsuperscript{23} \textit{Id.} ¶ 82.

\textsuperscript{24} CTIA is not arguing that revocation under Section 2.939 would be inappropriate in all cases. There may be circumstances, such as harmful RF interference, where revocation of equipment authorizations would meet the requirements of Section 2.939. In this case, however, revocation would go beyond the sorts of circumstances contemplated by Rule 2.939 and would harm consumers.
The Commission’s equipment authorization regime serves as the certification process for millions of products currently in the hands of U.S. consumers. The device ecosystem is complex and even more complex when considering component parts, whether in cars, computers, tablets, and other connected devices, and the NPRM does not account for the potential unintended consequences that revocation would cause across the entire ICT economy given these complexities. Requiring manufacturers to retroactively switch out covered component parts would be difficult, if not impossible, to do and risks jeopardizing supply chains and undermining innovation, while in many cases yielding no corresponding national security benefits.

Revocations as contemplated in the NPRM would likely directly harm American consumers. Devices manufactured whole or in part by Covered List companies are already integrated into consumers’ daily lives and are made available to consumers through many varied retail channels. Revoking existing authorizations for consumer products without a mechanism for removing them from the market will create significant confusion for consumers, who are likely unfamiliar with the FCC’s equipment authorization requirements, and could pass significant costs on to consumers who would presumably be placed in the difficult position of needing to replace newly unauthorized devices. Building a mechanism to remove retroactively de-authorized devices from the market would be complex and would need to consider how consumers would be made aware of the need to replace any particular device and what happens should a consumer choose not to replace the devices on which they currently rely, including those that continue to be used and connected to the internet ecosystem through other access points beyond carrier networks such as Wi-Fi, in addition to determining how any formal replacement process would be funded, which would likely require a legislative solution. Owners of de-authorized devices may also have trouble getting software updates or security patches for
those devices, leaving them more vulnerable to malicious attacks. Revocation thus stands to create a new category of vulnerable devices.

Wireless handsets enabled by cellular technology, in particular, illustrate significant implementation questions for the revocation proposal. The NPRM does not specify whether handsets are considered “covered” equipment, but the proposed rules suggest they could be, and the Commission appears to have reached the same conclusion in the USF “rip and replace” proceeding.\(^{25}\) If the FCC deems handsets “covered” equipment and revokes existing equipment authorizations, the FCC would create substantial uncertainty in the market about obligations with respect to handsets and what handsets will be able to lawfully operate.\(^{26}\) Further, federal communications policy to date has encouraged and sought to facilitate consumers’ ability to bring their own devices to connect to cellular networks; a new federal policy that prohibits certain end user equipment (particularly retroactively) would undermine that approach.\(^{27}\)

Further, the proposal could cause confusion and consume limited resources as the Commission moves forward in the USF rip and replace proceeding. The Commission has taken numerous actions to implement detailed reimbursement policies for replacing Covered List equipment funded by the Commission’s USF programs.\(^{28}\) Revoking existing equipment authorizations threatens to inject complexity into this effort, particularly if the Commission


\(^{26}\) Moreover, while these devices remained in consumer hands, even if they were unable to access carrier networks, they could still connect to the Internet, and thus could continue to be operated by consumers.

\(^{27}\) See, e.g., 47 C.F.R. §§ 27.16(e) (prohibiting handset locking by licensees in the Upper 700 MHz C Block), 54.202(a)(3) (establishing a commitment to comply with CTIA’s Consumer Code—which requires handset unlocking—as a safe harbor for an eligible telecommunications carrier’s obligation to demonstrate that it will “satisfy applicable consumer protection and service quality standards”).

\(^{28}\) See FCC, Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, https://www.fcc.gov/supplychain.
revokes authorizations for a universe of equipment that is broader than, or inconsistent with, the equipment targeted by the USF rip and replace proceeding. The Commission should be careful not to slow or undermine the important work of its rip and replace program.

Retroactive revocation may also weaken supply chains by impacting mutual recognition agreements ("MRA") that industry relies on to facilitate trade in telecommunications equipment. MRAs allow participating countries to agree to accept the test results and/or product approvals performed by the Conformity Assessment Bodies of the other country, thus reducing burdens on manufacturers and speeding time to market. Revocations by the FCC could undermine the MRA construct or frustrate their ongoing administration. For example, the MRA between the European Community and the United States requires "confidence in the continued reliability of the other Party’s conformity assessments." Drastically altering the purpose and scope of the Commission’s equipment authorization process could raise questions about the predictability of U.S. conformity assessments.

The complexities and difficulties raised by the Commission’s proposal suggest that the agency should not take action on revocation for covered equipment, if at all, until it has time to take more input. Revocation of equipment authorizations for covered equipment would challenge the traditional and well-settled presumption against retroactive action and raises complicated questions that at a minimum will require far more examination than is possible on

---


the basis of this NPRM alone.\footnote{See 5 U.S.C. § 553(b) (requiring notice of proposed rulemaking prior to the adoption of a rule); \textit{International Union, United Mine Workers of America v. Mine Safety & Health Administration}, 407 F.3d 1250, 1259 (D.C. Cir.2005) ("[The APA’s] notice requirements are designed (1) to ensure that agency regulations are tested via exposure to diverse public comment, (2) to ensure fairness to affected parties, and (3) to give affected parties an opportunity to develop evidence in the record to support their objections to the rule and thereby enhance the quality of judicial review.") (citation omitted); \textit{Env’t Integrity Project v. E.P.A.}, 425 F.3d 992, 996 (D.C. Cir. 2005) (explaining that, “[g]iven the strictures of notice-and-comment rulemaking, an agency’s proposed rule and its final rule may differ only insofar as the latter is a ‘logical outgrowth’ of the former,” and that the logical outgrowth doctrine does not apply “where interested parties would have had to divine the agency’s unspoken thoughts . . . because the final rule was surprisingly distant from the Agency’s proposal”) (citations and quotation marks omitted).} After receiving and reviewing additional input, should the Commission decide to move forward with revocation, it should proceed following a risk-based approach that addresses those devices that threaten national security and impose safeguards to minimize the impact that could be caused by revocation of consumer devices. For example, the Commission should ensure that there is an adequate “runway” for decommissioning devices that are already in the market at the time of revocation, ensure that carriers can adequately support devices until they are phased out (e.g., through security patching) to mitigate the risk of these devices becoming less secure or targets for bad actors, and address how the process will be funded.

\subsection*{B. The Proposed Bidding Certification Should Be More Tailored.}

Aside from changes to the equipment authorization regime, the NPRM proposes new requirements for competitive bidding applications that may prove burdensome. To date, the Commission has generally required applicants for spectrum auctions to provide narrowly tailored certifications that are clear and simple to confirm.\footnote{See, e.g., 47 C.F.R. §§ 1.2105(a)(2)(vi), (vii), (xi), (xiii) (requiring bidders to make simple certifications regarding foreign ownership, joint bidding arrangements, prior defaults on Commission licenses, etc.).} The NPRM takes a new tack, proposing to require competitive bidding applicants to “certify that [their] bids do not and will not rely on financial support from any entity that the Commission has designated under Section 54.9 of its...
rules as a national security threat to the integrity of communications networks or the communications supply chain.\textsuperscript{34}

CTIA has been a champion of the Commission’s work to make spectrum available timely and efficiently. Successful auctions require clear and predictable rules and procedures for eligibility and the conduct of auctions. The proposed certification may cause compliance challenges for potential auction bidders because it is overly vague. For instance, an applicant would be required to certify that “its bids do not and will not rely on financial support from any entity” posing a national security threat. It is unclear what “rely on” and “financial support” mean in this context, which exposes bidders to uncertainty about their submissions. It can be difficult to trace the ultimate origin of financial support and it is not clear from the NPRM what a bidder would need to do to ensure that its bids do not “rely on” forbidden financial support. Entities that have received an investment from private equity, for example, may be unable to certify that they are not “relying” on any “financial support” from an entity that has been designated as problematic. Without a defined threshold of “support,” it may be difficult for a publicly traded company to confidently certify that it is not “relying on financial support” from a forbidden entity.

There are more targeted ways to address foreign investment, and the federal government has processes to address concerns. Notably, auction applicants are already required to disclose all parties holding indirect ownership interest in the applicant equaling 10% or greater, which would likely expose the kind of “distortionary financing” about which the Commission appears to be concerned. If the Commission nevertheless moves forward with requiring a new certification, at a minimum, it should revise the proposed certification to provide clarity and

\textsuperscript{34} Id. ¶ 96.
predictability to prospective auction applicants. For example, the Commission could specify a
disclosure threshold of 10% for “financial support” prospective bidders receive from designated
entities that have been deemed to pose a national security threat under the Commission’s USF
support restriction in Section 54.9 of the rules.35

Any bidding certification requirements should be narrowly tailored, clearly articulated,
and tied to promoting competition. Otherwise, as with the proposed certification here, the
Commission risks artificially limiting the number of applicants and undermining the fundamental
benefit of spectrum auctions: “allow[ing] market forces to determine the highest and best use of
scarce spectrum.”36

C. The NPRM Raises Several Compliance Challenges for Participants in and
Beneficiaries of the Equipment Authorization Regime.

The NPRM sets out several broad proposals, beyond revocation and bidding
certifications, that raise complex issues and, if enacted, may create unintended consequences.
While closing the “loophole” that currently permits companies on the Covered List to obtain
prospective equipment authorizations is a laudable goal,37 the NPRM’s approach may impose
unnecessary burdens on good actors within the ICT sector.

“Parts List.” The NPRM’s focus on component parts, in particular, raises significant
concerns. The NPRM indicates that the Commission is considering requiring all manufacturers
to provide a “parts list” noting the manufacturer of each part in order to obtain certification.38 A
“parts list” requirement will impose substantial burdens on all applicants as connected devices

35 47 C.F.R. § 54.9.
36 Transforming the 2.5 GHz Band, Report and Order, 34 FCC Red 5446, ¶ 22 (2019).
37 NPRM at Separate Statement of Commissioner Brendan Carr.
38 Id. ¶ 48.
today may have thousands of integrated components. Depending on how the obligation is structured, the parts list requirement could interfere with manufacturers’ ability to change components without additional approval, as they can today through the permissive change rules. Given the significant number of component parts inherent in modern devices and product development cycles, requiring reauthorization (or even resubmission of the parts list) every time a component part is changed would be unworkable. If the Commission were to pursue this approach, at a minimum, it should devise a workaround to permit minor changes without requiring new filings and delays each time a minor component is replaced.

Moreover, it is unclear how a parts list requirement would further the Commission’s national security goals because numerous component parts have no implications for radiofrequency interference or for national security. The Commission should be careful to not impose restrictions on industry where, as here, the corresponding benefits appear to be minimal at best.

**Attestation Requirements.** New proposed attestation requirements also raise significant questions that are not addressed in the NPRM, particularly given uncertainties about how the Commission will define and regulate component parts. In order to make accurate representations, applicants will need more clarity about what the Commission considers to be component parts and the reach of the definitions “telecommunications equipment” and “video surveillance equipment” as used in the current Covered Equipment list. The Commission seems to recognize the need for clarity but suggests that OET and the Public Safety and Homeland Security Bureau (“PSHSB”) can work out the details, perhaps in guidance or knowledge

---

39 See 47 C.F.R. § 2.1043. If anything, requiring a parts list would conflict with the Administration’s efforts to increase supply chain diversity by restricting manufacturers’ ability to swap out components.
database system ("KDB") bulletins.\textsuperscript{40} The Commission should clarify any new attestation obligations in final rules adopted in this proceeding.

\textit{Additional Public Comment.} The NPRM proposes to collect public comment on certification grants to "inform the Commission as to whether particular [covered] equipment inadvertently received a grant."\textsuperscript{41} Such an approach could encourage anti-competitive behavior, as it would allow companies to abuse the post-grant review process to delay authorizations for competitors. TCBs would be left in the position of adjudicating legal and national security issues rather than analyzing technical information related to RF concerns. If it moves forward with this proposal, the Commission should clarify the process, what information will be required, how confidentiality will be maintained, and how the Commission will safeguard against abuse.

D. \textbf{It is Vital that The Commission Account for the Costs and Benefits of Changes to Its Equipment Authorization Regime.}

The NPRM opts not to engage in a "conventional cost-benefit analysis."\textsuperscript{42} Where, as here, the costs of the proposed changes are likely to be far-reaching, a cost-benefit analysis is critical.\textsuperscript{43} To determine the best path forward, the Commission should address the burdens that

\begin{footnotesize}
\begin{enumerate}
\item \textsuperscript{40} NPRM ¶ 55.
\item \textsuperscript{41} Id. ¶ 50.
\item \textsuperscript{42} Id. ¶ 69.
\item \textsuperscript{43} The Commission concludes that a cost-benefit analysis is not "called for" because the FCC has "no discretion" to second-guess the decisions of other agencies on whether to place certain equipment on the Covered List. \textit{Id.} ¶¶ 70-71. While it is correct that the Commission lacks the national security expertise or authority to override or second-guess these agencies' determinations, these decisions are just one of the complex considerations raised by the Commission's proposals. Moreover, now that the Fifth Circuit has confirmed the FCC's authority to make "limited, communications-focused judgment[s]" in the realm of national security, \textit{Huawei}, 2 F.4th at 443, the Commission cannot avoid doing a cost-benefit analysis of its the equipment authorization proposals, particularly where, as here, no agency has undertaken the cost-benefit analysis that the NPRM eschews.
\end{enumerate}
\end{footnotesize}
its proposals would impose on manufacturers, applicants, agency staff, and consumers. Against this, the Commission should weigh the national security benefits that it expects to follow.

Although the proposed rules in Appendix A appear narrow in scope, their reach is likely to be broad, imposing delays, costs, and other burdens on American companies, TCBs, and the OET. The equipment authorization regime is vast. As the Commission acknowledges, with few exceptions, “for an RF device to be marketed or operated in the United States, it must have been authorized for use through” either certification or Supplier’s Declaration of Conformity (“SDoC”) procedures.44 And given the rapidly expanding IoT market, “the number of devices now being authorized has expanded into the millions[.]”45 Changes to the rules and processing procedures thus stand to impact myriad devices, ranging from garage door openers to the newest 5G end user devices. To the extent a rule change causes even minimal delays, numerous devices and stakeholders may be affected and costs may increase substantially for devices and technology.46 These challenges are compounded by the fact that the NPRM’s proposal does not tailor administrative burdens to risk. For instance, network equipment poses much different national security risks than consumer end devices, yet the NPRM treats them all equally with respect to the proposed changes to the equipment authorization regime.

In addition, the NPRM contemplates imposing compliance obligations on all equipment authorization applicants, not just the entities on the Covered List. The NPRM would require all equipment authorization applicants to make a certification that equipment (including any

---

44 NPRM ¶ 27.
45 Id. ¶ 25.
46 As noted above, to the extent the NPRM extends proposals to component parts, these costs and complexities would multiply.
component part) is not “covered equipment.” Likewise, the terms of Section 1.50002, which defines the Covered List, are broad, and may encompass a broad swath of equipment. Any equipment may be added to the List that, among other things, “is capable of . . . posing an unacceptable risk to the national security of the United States or the security and safety of United States persons.”

The Commission’s proposals go beyond a narrow and prospective limitation on equipment authorization for Covered companies. While the proposed rules in Appendix A to the NPRM would implement the prohibition on authorization for covered equipment and the applicant’s attestation that proffered equipment is not covered, the NPRM includes other proposals that will have broad impact on the entire equipment authorization regime. For example, the NPRM seeks comment on revoking existing equipment authorizations, requiring “parts lists” with certification applications, changing the SDoC eligibility requirements, and requiring TCBs to engage in more post-market surveillance, among others. Widespread prospective changes to the equipment authorization regime would create risks for U.S. supply chains, which could prove costly for manufacturers and consumers alike.

Finally, the NPRM would place substantial new responsibilities on OET and TCBs. The NPRM indicates that TCBs may implement the proposed prohibition on certification of “covered” equipment, with to-be determined guidance from OET. The NPRM also proposes involving TCBs in post-grant reviews and analysis of information brought by “interested parties”

---

47 NPRM ¶ 47 and Appendix A, Proposed Rules, § 2.911(d).
48 47 C.F.R. § 1.50002(b)(2)(iii).
49 NPRM ¶¶ 82-89, 48, 57-64, 51.
50 Id. ¶ 49.
that the grant should be set aside. It also would increase the scope of TCBs’ post-market surveillance. Absent additional resources and staffing, low-risk and no-risk equipment may face significant delays in obtaining approval; the cost of TCB services is likely to rise. As Acting Chairwoman Rosenworcel has noted, the FCC itself faces low numbers of engineers and budget constraints that hinder OET’s ability to address security issues. This all comes against the well-documented shortage of cybersecurity professionals in the United States’ workforce. The NPRM does not address any of this, from increases in TCB costs to how FCC budget and staffing will ensure that new duties do not slow the equipment authorization process.

E. Legal Issues in the NPRM May Make Alternative Approaches Preferable.

Historically, the FCC’s subject matter authority over equipment authorization has centered on spectrum management, such as limiting RF emissions and interference, and ensuring

51 Id. ¶ 50.
52 Id. ¶ 51.
53 TCBs charge various fees for their services. As one TCB explains, “[g]enerally speaking, one can expect to pay anywhere between $3,000 and $5,000 for FCC testing. However, testing for modules & more complex devices can be much costlier. In addition, it is important to take other expenses into consideration, such as the cost of labor. The total cost is also influenced by how extensive the testing process is.” Compliance Testing, LLC, Blog (May 13, 2021) https://compliancetesting.com/how-much-does-fcc-testing-cost/.
56 GAO as repeatedly made this observation: “OMB and our prior reports have pointed out that the federal government and private industry face a persistent shortage of cybersecurity and IT professionals to implement and oversee information security protections to combat cyber threats…. [T]he RAND Corporation and the Partnership for Public Service have reported on a nationwide shortage of cybersecurity experts in the federal government.” CGAO 19-144 CYBERSECURITY WORKFORCE: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs https://www.gao.gov/assets/gao-19-144.pdf
network interoperability. Congress also has directed the FCC to address accessibility. In the
NPRM, the Commission seeks comment on potential sources of legal authority for its proposal to
expand the equipment authorization regime to encompass national security.

The Commission is correct that its proposal to bar the authorization of equipment on the
Covered List “is not specifically authorized by the Secure Networks Act itself, pursuant to which
the Commission adopted the Covered List.” Notwithstanding, the NRPM posits that, “in order
to ensure that the Commission’s rules under the Secure Networks Act” are effective, “it is
necessary to rely on the Commission’s established equipment authorization procedures to restrict
further equipment authorization, and the importation and marketing, of such devices in the first
instance.” The Secure Networks Act was a directive law addressing the use of equipment in a
specific context: the use of federal funding provided through the Commission’s universal service
programs. Congress, well aware of the FCC’s targeted role in equipment regulation, did not
specifically direct the FCC to address policy objectives implicated by the legislation through
other means.

Given that Congress has spoken directly to the function of the Covered List and specified
a particular role for the Commission in the Secure Networks Act, it may be difficult for the
Commission to rely on general authority to do what the Secure Networks Act does not
specifically authorize. As CTIA explained in response to the Commission’s Further Notice of

---

57 NPRM ¶ 65.
58 Id.
60 Cf. Comcast Corp. v. FCC, 600 F.3d 642, 654 (D.C. Cir. 2010) (“Policy statements are just that—
statements of policy. They are not delegations of regulatory authority.”).
pre-empts more general remedies.”); Antonin Scalia & Bryan A. Garner, Reading Law: The Interpretation
Proposed Rulemaking in the USF supply chain proceeding, where the Commission proposed to expand the prohibition on use of covered equipment to “any communications company . . . regardless of whether they use universal service support to do so”\textsuperscript{62}—the Commission’s legal authority beyond conditioning USF support is “unclear at best.”\textsuperscript{63} The same is true here, where the Commission seeks a similar result by different means.

In light of the practical challenges identified above, and some uncertainties about legal grounding, the Commission should consider other ways to achieve its national security supply chain goals. The Commission can promote its goals through alternate paths that are tailored to avoid the unintended consequences the NPRM’s approaches may produce. The Commission could await further direction from Congress, which has also been active on these issues. Or the Commission could consider pausing new equipment authorization grants to entities on the Covered List or support discussions between federal policymakers and industry to foster greater understanding of the supply chain dynamics manufacturers face.

\textsuperscript{62} Protecting Against Nat’l Sec. Threats to the Commc’ns Supply Chain Through FCC Programs, Report and Order, Further Notice of Proposed Rulemaking, and Order, 34 FCC Red 11423, ¶ 131 (2019).

\textsuperscript{63} Comments of CTIA, WC Docket No. 18-89, at 13 (filed Feb. 3, 2020).
IV. WITH RESPECT TO THE NOI, THE COMMISSION SHOULD SUPPORT UNIFIED IOT SECURITY WORK IN PARTNERSHIP WITH THE PRIVATE SECTOR, AND REFRAIN FROM PURSUING DISRUPTIVE REGULATIONS.

In the NOI, the Commission seeks comment on how it can leverage the equipment authorization regime to "spur trustworthy innovation for more secure equipment."64 CTIA agrees with the Commission on the importance of improving "trust through the adoption of cybersecurity best practices in consumer devices."65 To achieve this goal, however, the Commission should recognize that a flexible, risk-based, and voluntary approach to device security and adoption of international and industry standards will yield the best results in securing IoT devices and protecting networks and end users. As CTIA and others have made clear, a static regulatory framework is ill-suited to address dynamic and complex cybersecurity issues.66 Moreover, NIST, in partnership with the wireless industry, has established itself as the leader in this space and should continue to champion its flexible approach, with support from the FCC and industry.


Fueled by the unprecedented power of 5G, the diverse IoT marketplace is growing,67 delivering transformational benefits to consumers. The rapid proliferation of Internet-connected devices

---

64 NOI ¶ 98.
65 Id. ¶ 3.
67 Unlike other sectors of the American economy, the global COVID-19 pandemic further spurred IoT growth. See Smart Policy to Secure Our Smart Future, CTA, at 4 (March 2021) ("Smart Policy White Paper") ("The pandemic has pushed the fast-forward button on tech adoption — from our homes to our work to our doctor’s offices.").
devices and rise of the IoT “bring the promise of enhanced business efficiencies and increased customer satisfaction.” The IoT will bring immense change, from conveniences that make life easier (smart appliances) to life-saving health management tools (wireless infusion pumps, health trackers) to revolutionary business efficiencies (enhanced asset and productivity monitoring). Fundamentally, the IoT offers the potential to solve some of “the greatest social . . . challenges of our time,” including public health and environmental challenges.

The Commission should recognize the seismic benefits emerging from the IoT ecosystem. The emerging IoT ecosystem is making American lives easier and safer, particularly in the post-COVID-19 world. The NOI, however, focuses primarily on risk, positing that “[d]evices that operate as part of the IoT specifically raise concerns about security risks.” Addressing security in IoT is vital, but any action by the Commission should balance burdens with benefits to promote innovation and avoid embarking on counterproductive regulation.

---


71 See, e.g., Katerina Megas, More than just a milestone in the Botnet Roadmap towards more securable IoT devices, NIST Cybersecurity Insights (June 1, 2020), https://www.nist.gov/blogs/cybersecurity-insights/more-just-milestone-botnet-roadmap-towards-more-securable-iot-devices (“Internet of Things (IoT) devices offer tremendous capabilities to users. Looking around I see more and more ways, especially in a post COVID-19 world, that these devices will make our lives easier and safer, which makes this work more critical than ever.”).

72 NOI ¶ 100.

The wireless industry is a vital partner in ongoing efforts across the federal government to secure the IoT ecosystem. NIST has dedicated years to IoT security, and CTIA has partnered with NIST every step of the way. NIST should continue to lead the federal government’s work on IoT security with support from the FCC and other agencies. NIST’s non-regulatory nature, flexible, risk-based approach to cybersecurity, and dedication to collaboration with a diverse range of stakeholders make it well suited for this role.

NIST, in partnership with CTIA, publishes an extensive body of work on IoT security. For example, as the NOI notes, NIST published NISTIR 8259 in May 2020, which focuses on manufacturer activities and is part of NIST’s “two-pronged approach” to device security guidance. The companion piece, NISTIR 8259A (the “Core Baseline”), which establishes a core baseline of security capabilities that can serve as a default for minimally securable devices, is a voluntary and flexible document rooted in risk management. The Core Baseline is a “starting point” for organizations to use “in identifying the device cybersecurity capabilities for

---

73 These efforts include, among others, the DHS ICT SCRM Task Force, supra note 11; President Biden’s Executive Order on Improving the Nation’s Cybersecurity, which tasked numerous agencies with modernizing national security defenses; NTIA’s C–SCRIP; NIST initiatives, guidance, and best practices; the Commerce Department’s interim final rule on ICTS transactions, https://www.govinfo.gov/content/pkg/FR-2021-01-19/pdf/2021-01234.pdf; export controls and related regimes intended to exclude certain bad actors from U.S. markets; the Federal Acquisition Supply Council (“FASC”); CSRIC and NSTAC supply chain efforts; and the Cyberspace Solarium Commission.


75 NOI ¶ 101 (discussing NIST, Foundational Cybersecurity Activities for IoT Device Manufacturers, NISTIR 8259 (May 2020)).

new IoT devices they will manufacture, integrate, or acquire.”77 CTIA collaborated with NIST on the Core Baseline, which aligns with CTIA’s Cybersecurity Certification Test Plan for IoT Devices (“IoT Cybersecurity Certification Program”).78 More recently, NIST released NISTIR 8259B, the non-technical companion to the Core Baseline, which likewise provides a “starting point” for identifying non-technical supporting capabilities (e.g. documentation and education) to support IoT device cybersecurity.79

Congress has recognized the value of NIST’s expertise in IoT. In the IoT Cybersecurity Improvement Act of 2020, Congress directed NIST to develop standards and guidelines for federal agencies’ use of IoT devices.80 NIST, with CTIA’s involvement, is fulfilling its responsibilities under this law, including identifying cybersecurity criteria for a consumer IoT labeling pilot program.81 Likewise, multiple agencies are interested in IoT security, but as the

77 NIST, IoT Device Cybersecurity Capability Core Baseline, NISTIR 8259A, at ii (May 2020), https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259A.pdf. Other seminal NIST work includes NISTIR 8228, which is intended “to help federal agencies and other organizations better understand and manage the cybersecurity and privacy risks associated with their individual IoT devices throughout the devices’ lifecycles.” NIST, Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks, Internal Report 8228 (June 2019).

78 See Core Baseline at 5-10 (citing CTIA’s Certification Program as an “IoT Reference Example”). CTIA also worked with NIST on security guidance for consumer IoT and IoT used by the federal government. See NIST, Workshop Summary Report for “Cybersecurity Risks in Consumer Home Internet of Things (IoT) Devices” Virtual Workshop, Internal Report 8333 (March 2021) (describing NIST’s work with respect to consumer home IoT device security); NIST, Workshop Summary for “Building the Federal Profile for IoT Device Cybersecurity,” Internal Report 8322 (Jan. 2021) (listing CTIA as a presenter at NIST’s Federal Profile workshop). Work is still underway to define an international standard on IoT baseline security requirements at JTC1 ISO/IEC, with NIST contributing via the U.S. national body, as industry standardization progresses.


81 To this end, NIST recently released Draft Baseline Security Criteria for Consumer IoT Devices, and held a workshop on its efforts, representing key steps toward initiating the IoT labeling pilot program as directed by the Cyber EO. See NIST, Draft Baseline Security Criteria for Consumer IoT Devices (Aug. 31, 2021), https://www.nist.gov/system/files/documents/2021/08/31/IoT%20White%20Paper%20-
Consumer Technology Association ("CTA") notes, "they have rightly refrained from rigidly regulating it. Rather, agencies have focused on research, best practices and information sharing, among other things."82 The FCC should likewise consider how to support the workstreams of its federal partners and engage in inter-agency coordination to define voluntary standards rather than creating a fragmented regulatory approach.

Inter-agency coordination at the federal level is particularly vital because any FCC activity on IoT security must take into account dynamic international issues, which underscore the need for a unified federal approach that champions flexibility and global reciprocity, so that U.S. companies can make and sell electronic devices and services globally. As U.S. policymakers champion economic competitiveness and supply chain diversity, it is vital that government avoid fragmenting global markets or create trade barriers based on technical standards. Indeed, several countries are developing IoT policies and considering how to encourage cybersecurity. Many are looking to follow NIST's voluntary, flexible approach.83 Japan, for example, has leaned heavily on NIST's guidance and others may soon follow suit.84 Europe takes a more regulatory approach, adopting standards that will inform regional and

---

national requirements. The Commission should promote widespread adoption of NIST’s flexible work on a global scale rather than turning inward and imposing new prescriptive mandates.

A prescriptive approach to cybersecurity, implemented through the Commission’s equipment authorization process would be premature, but also potentially harmful by unsettling reliance on MRAs as discussed above. Rather than fostering a patchwork of international approaches, the Commission should support NIST’s efforts by engaging with the European Union and others to ensure harmonized global cybersecurity approaches that facilitate American leadership and innovation.

C. IoT Security Is Best Addressed Through Flexible, Voluntary, and Risk-Based Solutions.

1. There Is No One-Size-Fits-All Solution to Device Security.

Risk-management and flexibility must be the touchstones of any federal approach to IoT security. Different devices—from low- to high-complexity, managed to unmanaged, and home to federal government-use—deployed in different environments for different use cases will need different, flexible approaches to cybersecurity. Connected dog collars, for example, need not be held to the same security standard as connected pacemakers or industrial control systems. Instead, security approaches should be tailored to different devices, use cases, means of connectivity, and environments.

---


86 See Section III.A., supra.

87 NISTIR 8259 at 14 (“Since device cybersecurity capabilities will be decided and shaped by customer and use case context, different IoT devices will need different sets of device cybersecurity capabilities.”).
Leaders in the effort to secure the IoT ecosystem recognize this need for voluntary, flexible, and risk-based approaches. NIST’s Core Baseline makes clear that the core cybersecurity capabilities it identifies “will often need to be added or removed from an IoT device’s design, integration, or acquisition to best address an organization’s common cybersecurity risks.”

CTIA’s IoT Cybersecurity Certification Program likewise accommodates the security needs of different devices by using a voluntary, tiered approach for certification.

The NOI by contrast, suggests a more monolithic approach. Although the Commission solicits comment on “utiliz[ing] the equipment authorization process to incentivize better cybersecurity practices, either for all devices or specifically for IoT devices,” the better path would recognize that security considerations for IoT are distinct from those facing conventional ICT devices, including smartphones. Indeed, NIST and Congress have acknowledged that smartphones and laptops should not be treated the same as IoT for cybersecurity purposes.

They further recognized that security capabilities should be evaluated holistically, at the finished-product functional level, as opposed to the component or sub-assembly level. The Commission should likewise avoid attempting to develop regulatory solutions for all devices.

2. Cybersecurity Is Ill-suited for Static, Regulatory Approaches.

In the NOI, the Commission asks “what form should . . . provisions [to utilize the equipment authorization process to incentivize better cybersecurity practices] take and how

---

88 NISTIR 8259A at 3.
90 NOI ¶ 102 (emphasis added).
91 See NISTIR 8228 at 29; NISTIR 8259 at 1; IoT Cybersecurity Improvement Act § 2(4)(A).
92 Id.
would such a program be structured most effectively,” as well as questions about specific
“technologies or cybersecurity methods that mitigate security risks (e.g., RF fingerprinting or
some other method).” A static regulatory model, with prescriptive rules requiring specific
technologies or controls, is the wrong approach to cybersecurity in general, including IoT device
security. First and foremost, static requirements are incompatible with the complex, dynamic,
and rapidly evolving nature of cybersecurity threats.

Further, prescriptive requirements can do more harm than good, providing a road map for
hackers and encouraging a check-the-box, compliance mindset, which does not encourage the
proactive approaches required to stay ahead of bad actors. Moreover, addressing cybersecurity
through the equipment authorization model risks putting too much focus on device-centric
capabilities, without proper consideration of the broader security context in which devices
operate. How devices interact with other devices, systems, and environments should be
considered when identifying reasonable cybersecurity features to incorporate in any single
device. There are also factors beyond the device hardware—including software development,
updates, network security, and the existence of Mobile Device Management solutions—that must
factor into the equation. The equipment authorization process is not equipped to analyze and
address such complex considerations.

---

93 NOI ¶ 102.

94 See Smart Policy White Paper at 4 ("While cybersecurity is increasingly recognized as a business and
operational imperative, it is a technical challenge that shifts over time due to rapidly changing technology
and dynamic threats and attack techniques. Federal legislators, regulatory agencies, and state and local
governments are not equipped to regulate this broad technical challenge—at least, not alone.").

95 See Draft Labeling Criteria White Paper at 1 (recognizing that providers and customers should be able
to choose “the best solutions for their devices and environments” as “[o]ne size may not fit all”).
For these reasons, industry and the federal government historically have rejected static and prescriptive rules related to cybersecurity.\textsuperscript{96} The NIST Core Baseline strives to identify the “what” of IoT device security, but it does not seek to define the “how.” By “not specify[ing] how the device cybersecurity capabilities are to be achieved, . . . organizations . . . have considerable flexibility in implementing [the Core Baseline] to effectively address needs.”\textsuperscript{97} Similarly, the CTIA IoT Cybersecurity Certification Program makes clear that “[m]any different mechanisms may be used to achieve the security goals.”\textsuperscript{98} CTIA urges the Commission likewise to refrain from regulatory or prescriptive approaches to device security.

Relatedly, the Commission should not take existing guidance and transform it into regulation. The NOI asks whether the Commission should “encourage manufacturers of IoT devices to follow the guidance in [NISTIR 8259][.]”\textsuperscript{99} To the extent that this “encouragement” would tie the NIST guidance to the equipment authorization process, CTIA urges against this approach. NIST’s voluntary, flexible, and risk-based guidance was not designed to be codified into regulation. NISTIR 8259 offers recommendations for certain “foundational cybersecurity activities that manufacturers should \textit{consider} performing,” noting that “[t]he considerations mentioned within these activities may not apply to all customers or manufacturers, but others may find the same considerations to be vital.”\textsuperscript{100} Similarly, the Core Baseline makes clear that it “is intended to give all organizations a starting point for IoT device cybersecurity risk

\textsuperscript{96} \textit{Smart Policy White Paper} at 4 (quoting the FTC and the Department of Commerce discussing the risks associates with premature or prescriptive IoT regulation).

\textsuperscript{97} NISTIR 8259A at 3 (emphasis added).

\textsuperscript{98} CTIA IoT Cybersecurity Certification Program, Test Plan, § 1.2.

\textsuperscript{99} See NOI ¶ 102.

\textsuperscript{100} NISTIR 8259 at v, 17 (emphasis added).
management, but the implementation of all capabilities is not considered mandatory” and that “[t]he individual capabilities in the baseline may be implemented in full, in part, or not at all.”\textsuperscript{101} Were such guidance even legally suitable for codification,\textsuperscript{102} doing so will undermine its intended flexibility and jeopardize device security.


While NIST has been developing expertise in cybersecurity and using that expertise to craft voluntary, risk-based guidance for IoT manufacturers and users, the FCC has not had occasion to acquire substantial expertise or personnel with deep knowledge of hardware, firmware, development practices, product and system updates, digital identity solutions, and myriad other issues. This, combined with the Commission’s lack of staffing and resources,\textsuperscript{103} counsel caution about the imposition of new cybersecurity requirements within the Commission’s equipment authorization regime. Indeed, OET staffing has steadily declined since 2014, and the 2022 budget does not appear to contemplate additional personnel or resources.\textsuperscript{104} The sheer volume of connected devices that will pass through the regime in the coming years will only exacerbate these resource deficiencies.

Any requirements will also have implications for enforcement and rulemaking resources; violations or misrepresentations may need to be investigated by the Enforcement Bureau; and

\textsuperscript{101} NISTIR 8259A at 1-2 (emphasis added).
\textsuperscript{102} See Emily S. Bremer, Incorporation by Reference in an Open-Government Age, 36 Harv. J.L. & Pub. Pol’y 131, 202 (2013) (“Material may also be inappropriate for incorporation by reference into regulation “if it uses voluntary or advisory, rather than mandatory, language.”).
\textsuperscript{103} See Rosenworcel March 10 Testimony at 4-5 (explaining that the FCC has not committed “any resources to tackling … cybersecurity and specifically securing 5G networks and supply chains” and noting that “less than one percent of [the FCC’s] budget is set aside for new technology for [OET]”).
further rule refinements will tax the Office of the General Counsel and other resources. These efforts likewise will need cybersecurity capacity and depth of experience that may not be present now in the agency. Thus, even if a regulatory approach to cybersecurity was appropriate or advisable from a policy perspective—which it is not—the Commission is simply not resourced to create, implement, and manage a new equipment cybersecurity regime.


While a flexible, risk-based approach to IoT device security—led by NIST—will foster a more secure IoT ecosystem, the Commission can complement NIST’s efforts and meaningfully contribute to IoT device security.

For example, leveraging its expertise related to communications networks, the Commission could task the newly re-chartered CSRIC to study many of the questions asked in the NOI. The Commission has successfully utilized a similar approach in the past. In 2015, CSRIC IV, Working Group 4, developed implementation guidance for NIST’s Cybersecurity Framework for each of the five key segments of the communications industry. CSRIC VIII has been rechartered to look at 5G security as a primary focus, and can be a valuable resource to help the Commission identify innovation and consider how it can support security in 5G and IoT. The Commission should consider asking CSRIC VIII to engage in a similar exercise for NIST’s IoT guidance or other applicable security baseline approaches to the communications sector. In so doing, the Commission should consider IoT workstreams in CSRIC that explore

---

risk-based approaches to the entire IoT ecosystem, taking into account the fact that the devices vetted and managed by communications services providers are only a small part of the IoT ecosystem. By contrast, service providers’ networks and their customers may be put at risk by insecure IoT devices that consumers connect to WiFi or other unregulated networks.107

More broadly, the FCC can focus on education about IoT device security for both the communications sector and consumers, perhaps in collaboration with NIST and the FTC as part of the Cyber EO’s IoT Labeling Pilot Program. Consumers need support to improve basic cyber hygiene and be responsible digital citizens that use secure password practices and accepted devices. CTIA has seen how effective consumer education campaigns can be, as with past smartphone theft prevention efforts.108 Likewise, the Commission, in coordination with other agencies, could explore supporting liability protections for innovations in security. Safe harbors, for example, can protect manufacturers, certification bodies, and other stakeholders from complex legal risks associated with making representations about device security. Such initiatives would further the Commission’s important goal of protecting U.S. communications networks without undermining NIST’s efforts to create voluntary, flexible, risk-based guidance.

107 See Wi-Fi Alliance, Wi-Fi predictions for 2021, https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-wi-fi-predictions-for-2021 (explaining that “[t]he number of devices connected to the internet, including machines, sensors, and smart home devices is forecast to reach 41.6 billion in the next four years”); Wi-Fi Alliance, Wi-Fi predictions from Cisco’s Annual Internet Report (Mar. 18, 2020), https://www.wi-fi.org/beacon/the-beacon/wi-fi-predictions-from-cisco-s-annual-internet-report (estimating that by 2023, there will be 628 million public Wi-Fi hotspots worldwide, up from 169 million in 2018).

E. The Communications Act Does Not Authorize the FCC to Pursue the Cybersecurity Proposals Set Forth in the NOI.

The Commission’s proposal lacks solid grounding in legal authority. The FCC does not purport to identify legal authority for adding cybersecurity-related requirements to the equipment authorization rules, but presumably the Commission would rely on some of the same legal authorities it cites to support proposed changes in the NPRM: the Secure Networks Act, Sections 302 and 303(e) of the Communications Act, and the Communications Assistance for Law Enforcement Act ("CALEA"). None of these provisions authorizes such requirements.

The Secure Networks Act does not authorize the proposed cybersecurity requirements. The Act is focused on eliminating the use of federal USF funding for equipment on the Covered List.\textsuperscript{109} If the Secure Networks Act does not authorize expanding the USF-related prohibition to the communications market as a whole—as the Commission admits it does not\textsuperscript{110}—the Act plainly does not authorize the Commission to impose regulatory requirements related to cybersecurity on the vast IoT ecosystem. Nor would incorporating cybersecurity obligations into the equipment authorization regime fulfill the Commission’s responsibilities in the Secure Network Acts; such regulations would be, impermissibly, “ancillary to nothing.”\textsuperscript{111}

Neither Section 302 nor Section 303(e) provide the requisite authority. As the Commission acknowledges, both of these provisions pertain to the technical aspects of radiofrequency emission. Section 302 authorizes the Commission, “consistent with the public interest, convenience, and necessity,” to “make reasonable regulations … governing the interference potential of devices which in their operation are capable of emitting radio frequency

\begin{itemize}
  \item \textsuperscript{109} 47 U.S.C. § 1602(a)(1).
  \item \textsuperscript{110} NPRM ¶ 65.
  \item \textsuperscript{111} Am. Libr. Ass’n v. FCC, 406 F.3d 689, 700 (D.C. Cir. 2005).
\end{itemize}
energy." Section 303(e) authorizes the Commission to, “as public convenience, interest, or necessity requires . . . [r]egulate the kind of apparatus to be used with respect to its external effects and the purity and sharpness of the emissions from each station and from the apparatus therein.” Importantly, the references to the “public interest” in Section 302 and 303 are cabined by the language that follows, setting forth specific mandates for the Commission to carry out. Although the Commission acknowledges that its “authorization processes are primarily for the purpose of evaluating equipment’s compliance with technical specifications intended to minimize the interference potential of devices that emit RF energy,” the Commission nonetheless suggests that these provisions establish authority to alter the equipment authorization regime to serve the policy objectives set forth in the item. This assertion lacks merit.

The “public interest” language in Sections 302 and 303(e) does not authorize the Commission to take actions that the statute does not permit. As the D.C. Circuit has explained, “[t]he FCC cannot act in the ‘public interest’ if the agency does not otherwise have the authority to promulgate the regulations at issue. . . . The FCC must act pursuant to delegated authority before any ‘public interest’ inquiry is made.” A regulation requiring adherence to cybersecurity best practices addresses neither “the interference potential of [RF-emitting] devices” nor the “external effects and the purity and sharpness of the emissions” from such devices.

---

113 Id. § 303(e).
114 These provisions differ from Section 254, which arguably permits the Commission to consider the public interest more generally, in light of the purposes of the Act in determining how to distribute subsidies, which may include national security considerations. See Huawei, 2 F.4th at 437-442.
115 NPRM ¶ 66.
116 Motion Picture Ass’n of Am., Inc. v. FCC, 309 F.3d 796, 806 (D.C. Cir. 2002).
devices, and thus would fall wholly outside the scope of these statutes. While the Commission correctly notes, as addressed above, that the agency has imposed requirements through the equipment authorization to achieve “other statutory responsibilities,” no such statutory command exists here.

The Commission likewise cannot rely on CALEA to support new cybersecurity provisions as contemplated in the NOI. The NPRM suggests that CALEA may provide an “alternative basis for . . . security rules.” But here too, the Commission seeks to rely on a narrowly focused law to impose obligations that fall outside its scope. First, CALEA applies only to “telecommunications carriers.” Thus, devices that are not used for common carriage—including many IoT devices that appear to be at the heart of the NPRM & NOI—are beyond its reach. Second, the FCC’s authority to establish any requirements at all is limited: the Commission may only set “technical requirements or standards” where “industry associations or standard-setting organizations fail to issue technical requirements or standards.” Even then, the FCC can adopt standards only to “meet the assistance capability requirements” of the law: enabling the government to intercept communications. This capability is far narrower than the general cybersecurity requirements that the NOI contemplates. As CTIA has explained,

117 47 U.S.C. §§ 302a(a); 303(e).
118 NPRM ¶ 66.
119 See MPAA, 309 F.3d at 807 (“[Video description] rules [for broadcasters] may be highly salutary. But . . . [w]hat is determinative here is the FCC acted without delegated authority from Congress.”); cf. Am. Libr. Ass’n v. FCC, 406 F.3d 689, 702 (D.C. Cir. 2005) (rejecting FCC’s assertion of ancillary authority “because the disputed broadcast flag regulations rest on no apparent statutory foundation and, thus, appear to be ancillary to nothing).
120 Id. ¶ 68.
122 Id. § 1006(b) (emphasis added).
“Congress made the United States Attorney General responsible for the majority of [CALEA’s] implementation . . . CALEA does not support a broad role for the Commission even within CALEA’s targeted regulatory regime.”123

Fundamentally, expanding the equipment authorization program to include cybersecurity requirements is at odds with the Commission’s historical practice of affording proper deference to the expertise of other agencies in areas outside the Commission’s bailiwick. The deference typically afforded to federal agencies is minimized where the agency acts in an area in which it lacks expertise.124 In upholding the Commission’s USF supply chain order and rejecting arguments that the order exceeded the FCC’s authority, key to the Fifth Circuit’s analysis was the fact that the authority the Commission exercised “closely resemble[d] the kind of national security authority it has exercised for decades—limited, communications-focused judgment informed by expert agencies and deferential to their views.”125 In other areas outside of its expertise, the Commission has been similarly deferential.126 Although the NOI discusses

123 CTIA Supply Chain FNRPM Comments at 15.
124 See, e.g., Gonzales v. Oregon, 546 U.S. 243, 269 (2006) (“The deference here is tempered by the Attorney General’s lack of expertise in this area and the apparent absence of any consultation with anyone outside the Department of Justice who might aid in a reasoned judgment.”); Nat’l Treasury Empls. Union v. Fed. Lab. Rel. Auth., 712 F.2d 669, 673 (D.C. Cir. 1983) (“We note first that the FLRA’s decision turned on interpretation of MSPB regulations and case law, matters outside the Authority’s expertise and not within its enabling statute. Therefore the respect a court ordinarily accords to an agency's decision when the agency construes its own charter is not due here.”); cf. Nat’l Wildlife Fed’n v. Westphal, 116 F. Supp. 2d 49, 57 (D.D.C. 2000) (“When . . . an agency has made a determination that falls within its area of special expertise, deference is at its zenith.”).
125 Huawei Techs., 2 F.4th at 443.
126 See, e.g., Proposed Changes in the Comm'n’s Rules Regarding Hum. Exposure to Radiofrequency Electromagnetic Fields, Resolution of Notice of Inquiry, Section Report and Order, Notice of Proposed Rulemaking, and Memorandum Opinion and Order, 34 FCC Red. 11687, ¶ 153 (2019) (“[T]he Commission recognizes that it is not a health and safety agency, and necessarily gives considerable weight to the expertise of agencies and groups, like the FDA and IEEE, who can interpret the biological research necessary to assess the health impact of RF emissions and determine what exposure levels can be considered safe for humans.”).
cybersecurity work conducted by other agencies and seeks comment on leveraging those efforts, the proposal does not appear to contemplate a role for expert agencies in implementing and maintaining the regulatory regime the FCC seeks to adopt.

V. CONCLUSION.

As the Commission continues to think about national security, supply chain, and cybersecurity issues facing the communications sector, CTIA urges the Commission to appropriately account for the complexities of the industry and the needs of consumers, to encourage unified, risk-based policies that reflect ongoing and effective work in the private sector and at other agencies.

Respectfully submitted,

/s/ Melanie K. Tiano

Melanie K. Tiano
Assistant Vice President, Cybersecurity and Privacy

Thomas C. Power
Senior Vice President and General Counsel

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

John A. Marinho
Vice President, Technology and Cybersecurity

September 20, 2021

CTIA
1400 16th Street NW, Suite 600
Washington, D.C. 20036
202-736-3200