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, General Counsel

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

Justin Perkins
Manager, Cybersecurity and Policy

CTIA
1400 16th Street, NW, Suite 600
Washington, DC 20036
202-736-3200
www.ctia.org

April 7, 2023

Table of Contents

I. INTRODUCTION

CTIA[1] submits these comments in response to the Federal Communications Commission's ("FCC" or "Commission") Further Notice of Proposed Rulemaking ("FNPRM"), in the above-referenced proceeding, which considers additional changes to the equipment authorization regime to address equipment that may pose "an unacceptable risk to national security."[2] Specifically, in the FNPRM, the Commission seeks comment on additional issues related to the equipment authorization process, including whether to regulate component parts, whether to revoke existing equipment authorizations involving "covered" equipment, effects on the supply chain, requiring a U.S. point of presence for certified equipment, and other issues.[3] In addition to questions about the equipment authorization process, the Commission seeks comment on changes to the competitive bidding regime.

The Commission's objectives in this proceeding remain laudable. But as the FNPRM recognizes, implementing these objectives raises a host of challenges. As the FCC moves forward, CTIA urges the Commission to account for implementation complexities, avoid undue disruption for consumers and other stakeholders, and minimize regulatory burdens that could

[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.

[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, Report and Order, Order, and Further Notice of Proposed Rulemaking, ¶ 1 (rel. Nov. 25, 2022).

[3] *Id.* ¶¶ 267-332 ("FNPRM").

hinder innovation and harm consumers. Indeed, the Commission can work to ensure the risks identified by national security agencies are addressed in a targeted way, while minimizing impacts on end users and regulated entities.

Specifically, the Commission should (i) carefully consider the practical difficulties with parts list and attestation requirements for component parts, and avoid onerous obligations, (ii) refrain from adopting rules for revocation that would jeopardize consumer access to existing devices and technologies or cause confusion and uncertainty in the market, (iii) account for supply chain disruptions and consumer harm when implementing changes to the Covered List, (iv) avoid creating unnecessary costs and obligations on the equipment approval process, and (v) to the extent one is needed, design a more tailored bidding certification.

II. CTIA AND THE WIRELESS INDUSTRY REMAIN COMMITTED TO ENSURING THE SAFETY AND SECURITY OF U.S. WIRELESS NETWORKS.

The wireless industry continues to take steps to ensure that networks are safe, whether from "covered" equipment or other threats. Security is a necessary part of a fifth generation ("5G") wireless economy as well as a healthy Internet of Things ("IoT") industry. The wireless industry leads on information and communications technology ("ICT") security, assisting government and other stakeholders with deployment of risk-based solutions for U.S. networks.

CTIA has launched a variety of initiatives that promote secure wireless technology. Recently, CTIA launched its 5G Security Test Bed to provide government groups and the wireless and technology industries a real-world, practical environment to test recommendations

and security solutions for 5G, the most secure generation of wireless to date.[4] To help promote wireless network security, CTIA published a white paper on zero trust ("ZT") earlier this year.[5]

CTIA and its members are engaged in numerous efforts to promote network security, spanning myriad agencies, partnerships, and standards bodies. CTIA's Cybersecurity Working Group ("CSWG") convenes all parts of wireless—service providers, manufacturers, and wireless data, internet, and applications companies—to facilitate innovation, research, and cooperation in response to threats. Through the CSWG, CTIA and its members collaborate with federal partners, including the Commission, the Department of Homeland Security ("DHS"), the National Institute for Standards and Technology ("NIST"), and the White House. The Commission's Communications Security, Reliability, and Interoperability Council ("CSRIC") includes CTIA members, and CSRIC functions as a critical public-private collaboration on cybersecurity. CTIA and several members spearheaded the Cybersecurity & Infrastructure Security Agency's ("CISA") ICT Supply Chain Risk Management ("SCRM") Task Force to address cyber threats to ICT supply chains.[6] The President's National Security Telecommunications Advisory Committee ("NSTAC") convenes CTIA members to provide recommendations to the President.[7] CTIA's members help develop wireless standards in key

[4] 5G Security Test Bed Information Sheet, 5G Security Test Bed (June 14, 2022), https://5gsecuritytestbed.com/wp-content/uploads/2022/06/STB-One-Pager_061422.pdf.

[5] Defining Zero Trust: Industry Approaches and Policy Frameworks for Strong Wireless Network Security, CTIA (Jan. 9, 2023), https://www.ctia.org/news/defining-zero-trust-industry-approaches-and-policy-frameworks-for-strong-wireless-network-security.

[6] *ICT Supply Chain Risk Management Task Force*, CISA, https://www.cisa.gov/resources-tools/groups/ict-supply-chain-risk-management-task-force (last visited Mar. 30, 2023).

[7] *About the President's NSTAC*, CISA, https://www.cisa.gov/about-presidents-nstac (last visited Mar. 30, 2023).

standards bodies, such as the 3rd Generation Partnership Project ("3GPP"), to help ensure that no single country or company exerts undue influence as participants develop standards.[8]

III. ICT SECURITY DEMANDS A WHOLE-OF-GOVERNMENT APPROACH AND CAREFUL COORDINATION.

The United States needs a unified, risk-based approach to ICT security, and the Commission should avoid taking actions that will complicate or conflict with a comprehensive approach. That is particularly true given the structure created by the Secure Networks Act ("SNA") and Secure Equipment Act ("SEA"),[9] which places national security determinations in the hands of agencies that are best equipped to make those decisions, and charges the FCC with implementing the decisions made by the relevant agencies.

The FCC's role in this process is carefully considered. By entrusting implementation of the regulations with the Commission, Congress gave the agency the authority and obligation to ensure that national security threats are mitigated in a way that does not unduly harm or burden consumers or other stakeholders. Ensuring a "rapid, efficient, Nation-wide, and world-wide wire and radio communication service" remains the bedrock of the FCC's mission, and the actions that it takes to implement the Covered List must be driven by that core goal.[10]

The Commission should make clear that national uniformity is critical in implementing changes to the equipment authorization process. Determinations about which devices pose a national security threat, about how best to mitigate those threats, and about how to balance the

---

[8] *See* Tom Sawanobori, *Wireless Industry Already Tackling Cyber Risks Outlined by Recent Government Paper*, CTIA (May 10, 2021), https://www.ctia.org/news/blog-wireless-industry-already-tackling-cyber-risks-outlined-by-recent-government-paper.

[9] Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 133 Stat. 158 (2020) (codified as amended at 47 U.S.C. §§ 1601–1609) ("SNA"); Secure Equipment Act of 2021, Pub. L. No. 117-55, 135 Stat. 423 (2021) (codified at 47 U.S.C. § 1601) ("SEA").

[10] 47 U.S.C. § 151.

potentially competing federal objectives in ensuring security and widespread access to devices cannot be made at the state or local level. The FCC should emphasize that state or local actions seeking to establish different or additional requirements in this area would conflict with these federal objectives.

While CTIA discourages the use of revocation, the Commission should ensure that any authorization revocations that would apply to devices or equipment already sold and in the field are accompanied by appropriate compensation. As CTIA noted in its previous comments, any revocation by the FCC of authorizations for equipment or devices already in use could come with significant financial cost to network operators and consumers who have purchased equipment and devices based on the FCC's prior determination that they were approved for use in the United States.[11] Reversing a prior authorization can be significant, and, particularly for component parts, could become very complicated. Revoking prior equipment authorizations for finished products and components only should be undertaken with a full understanding of the costs and complexity involved in removing that equipment/device from the market, and after the FCC has developed a plan for how the government will compensate for the cost of replacement and installation of acceptable replacements.[12]

---

[11] Comments of CTIA, ET Docket No. 21-232, EA Docket No. 21-233, at 19 (Sept. 20, 2021), https://www.fcc.gov/ecfs/file/download/CTIA%20Comments%20FCC%20Equipment%20Authorization%20NPRM%20NOI%209.20.21.pdf?folder=10920609405781 ("Comments of CTIA").

[12] Any action on component parts or revocation that requires third parties to undertake costly changes or replace equipment must be compensated. The government in the recent past has recognized the need for compensation and incentives when taking action that requires changes to or replacement of equipment in place for national security reasons. The prime example is the $1.9 billion "rip and replace" program, the Secure and Trusted Communications Network Reimbursement Program ("Reimbursement Program") overseen by the Commission in response to congressional direction. The program was set up to reimburse providers for reasonable expenses incurred when removing, replacing, and disposing of communications equipment and services produced by certain covered entities from their networks. *See Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*,

Thus, as it moves forward with this proceeding, the FCC should provide clarity, minimize impacts on the national communications infrastructure, and plan for appropriate compensation in the rare circumstances where revocation is required. It should also promote a whole-of-government approach, ensure coordination with other agencies' efforts, and avoid making determinations that might interfere or conflict with decisions of other agencies.

IV. THE COMMISSION SHOULD BE CAUTIOUS ABOUT ANY REGULATIONS ADDRESSING COMPONENT PARTS.

Several questions in the FNPRM ask about whether and how the Commission might approach component parts or modules.[13] As reflected in comments on the earlier Notice of Proposed Rulemaking ("NPRM"),[14] expansion of Commission regulation beyond equipment that is specifically identified on the Covered List raises serious questions and challenges.

Second Report and Order, 35 FCC Rcd 14284 (2020) (adopting rules to implement the Reimbursement Program); *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Third Report and Order, 36 FCC Rcd 11958 (2021) (modifying the Reimbursement Program rules to incorporate the 2021 Consolidated Appropriations Act's amendments to the SNA). The absence of a similar congressional allocation or other mechanism for reimbursement here counsels against disruptive Commission action.

[13] FNPRM ¶¶ 268-87.

[14] *See, e.g.*, Comments of CTIA at 15-17; Comments of NCTA – The Internet & Television Association, ET Docket No. 21-232, EA Docket No. 21-233, at 4, 12 (Sept. 20, 2021), https://www.fcc.gov/ecfs/file/download/092021%2021-232%2021-233%20NCTA%20Supply%20Chain%20Equipment%20Authorization%20NPRM%20Comments.pdf?folder=109200439117705 ("Comments of NCTA"); Comments of NTCA – The Rural Broadband Association, ET Docket No. 21-232, EA Docket No. 21-233, at 4 (Sept. 20, 2021) https://www.fcc.gov/ecfs/file/download/09.20.21%20NTCA%20Comments%20ET%20Dkt%2021-232%20EA%20Dkt%2021-233.pdf?folder=10920058610398 ("Comments of NTCA"); Comments of The Consumer Technology Association, ET Docket No. 21-232, EA Docket No. 21-233 at 11-13, 16-17 (Sept. 20, 2021), https://www.fcc.gov/ecfs/file/download/CTA%20Equipment%20Authorization%20Comments.pdf?folder=10920131021049 ("Comments of CTA").

A. The Commission Should Not Introduce Parts Lists into the Equipment Authorization Process or Regulate Component Parts.

Sweeping "component parts" into the equipment authorization process would create a bevy of new practical hurdles. Parts lists for electronic equipment are complex. Electronic device components may be sourced from numerous companies, and the number of underlying components and levels of suppliers increases as a device's complexity and functionality increases. In addition, the component makeup of any given electronic device is proprietary and competitively sensitive.

A broad approach to component parts or a parts list, such as requiring verification of the original source of each of dozens of components, subassemblies, and subcomponents—for all equipment subject to FCC oversight—would be a significant burden. It would also raise substantial competitive concerns, potentially giving competitors access to valuable information about material sourcing and design. Given the wide range of component parts that have little or no impact on security issues, absent specific findings from national security agencies with respect to particular components, there would be little corresponding benefit to these burdens.

Even putting aside the cost and complexity of establishing systems to track parts, imposing such a requirement would put an additional drag on innovation. Requiring entities to track parts lists and seek recertification when parts change would disincentivize substitution and innovation, and impose additional demands on the already burdened Telecommunications Certification Bodies ("TCB") and FCC equipment authorization process.

Accordingly, the Commission should refrain from any steps that would require the creation and maintenance of parts lists as part of the equipment authorization process. If the Commission, however, decides that it should seek detailed information about component parts or supplier issues from applicants, it should treat such information as confidential, proprietary, and

exempt from public inspection, including by modifying 47 C.F.R. § 0.461 and 47 C.F.R. § 0.457(d) to ensure maintenance of confidential treatment.

For both practical and legal reasons, the FCC also should not, by itself, "attempt to identify ranges of components based on their risk assessment[s],"[15] and should instead rely on the whole-of-government effort that is working on these security issues. Independent FCC risk assessments of component parts would lead to needless complexity, as the agency would necessarily have to work through a cascading range of procedures to try and establish the risks posed by a near-infinite variety of component parts.

In addition to these practical concerns, the Commission lacks statutory guidance for such a process, which would require the agency to develop criteria from whole cloth for every part of every device that is subject to the Commission's rules. These are matters well outside the agency's traditional areas of expertise, a fact that the FCC's Covered List itself recognizes by referring to "communications equipment and services" that are "deemed to pose an unacceptable risk to the national security of the United States or the security and safety of United States persons, *based exclusively on any of four sources for such a determination*" that all lie outside the agency.[16]

Indeed, far from providing guidance on the factors that the FCC should use, the structure of the SNA and SEA entrusts the national security agencies with the authority to make judgments about what constitutes national security threats,[17] thereby recognizing that the

[15] FNPRM ¶ 279.

[16] *See* List of Equipment and Services Covered By Section 2 of The Secure Networks Act, FCC, https://www.fcc.gov/supplychain/coveredlist (last updated Sept. 20, 2022) (emphasis added); *see also* 47 C.F.R. § 1.50002.

[17] *See, e.g.*, SNA, §§ 2(b), (c) (stating that "The Commission *shall* place on the list," and directing that "in taking action under subsection (b)(1), the Commission *shall* place on the list any communications equipment or service that poses an unacceptable risk to the national security

Commission is not the proper entity to be making these determinations. If the Commission were to create its own risk assessment rubric and apply that to equipment that is *not* subject to the requisite finding by an appropriate agency, it runs the risk both of exceeding the FCC's authority and conflicting with the judgments made by the agencies that have the expertise, the express authority, and the access to intelligence information to make these determinations.

These issues become especially acute when applied to *existing* equipment. The challenge of creating parts lists for new authorizations is daunting, but these issues become even more intense for equipment that has already been approved and is currently in use or being sold in the marketplace. The FNPRM presents "requiring the particular components of equipment be replaced or certain security patches be implemented" as being potentially less intrusive alternatives "that might avoid the need to replace equipment that had been previously authorized[.]"[18] However, there may be no choice but to replace the entire finished good, which would represent a significant cost to consumers. Additionally, mandating identification and replacement of component parts would raise all of the same issues created by the revocation of authorizations, discussed in Section V, *infra*, as well as a host of complex problems associated with grafting new tracking and tracing obligations onto existing equipment and supplier relationships.

Lastly, there is no need for the FCC to duplicate the work being done by CISA's ICT SCRM Task Force.[19] The Commission should not try to turn the Task Force's efforts on a

---

of the United States or the security and safety of United States persons *based solely* on one or more of the following [enumerated] determinations," all of which come from outside the agency, generally including determinations made by national security agencies.) (emphasis added).

[18] FNPRM ¶ 302 (emphasis added).

[19] *ICT Supply Chain Risk Management Task Force*, CISA, https://www.cisa.gov/resources-tools/groups/ict-supply-chain-risk-management-task-force (last visited Mar. 30, 2023).

"hardware bills of materials" into regulatory or oversight burdens.[20] This work stream is ongoing and any guidance that is issued will be flexible and voluntary.[21] And the work of the Task Force serves to confirm the difficulty of a one-size-fits-all solution in examining elements beyond the finished product level. The Task Force is aiming only to provide a common taxonomy that could be useful in exchanging information, while emphasizing that such a tool is meant to be flexible and allow vendors to tailor it for their specific circumstances or use cases. Because of the uniqueness of each company's supply chain, there can be no common approach to addressing elements at a component level.

B. Any Component Parts Rules Should Be Crafted to Avoid Unnecessary Burdens on Consumers and Manufacturers.

If the Commission does decide to promulgate component parts rules, these rules should be reasonable and drafted to minimize the impact on consumers and manufacturers alike. Avoiding overly burdensome regulations will also allow for broader and quicker compliance. The Commission should also have reasonable expectations regarding the time it would take to source new component parts.

First, if new component manufacturers are added to the Covered List or existing Covered List entities' components are deemed "covered," the Commission should provide industry with at least two years to find replacement parts. A two-year timeline would allow companies to

[20] *See id.*

[21] *See* Press Release, CISA, ICT Supply Chain Risk Management Task Force Announces new members and Working Group, (Jan. 11, 2022), https://www.cisa.gov/news-events/news/ict-supply-chain-risk-management-task-force-announces-new-members-and-working ("The Hardware Bill of Materials Working Group will focus on identifying appropriate information for the development of a baseline hardware bill of materials template that organizations *can* use when procuring or deploying ICT products.") (emphasis added).

source, contract for, and test the replacement components, as well as receive authorization for the new components and/or modules.

Second, should the Commission decide to regulate component parts, it should do so in a manner that clearly communicates which components raise concerns. The agency should not put the burden on applicants or consumers to make judgment calls about which component parts do or do not fall within the scope of the FCC's regulation. That would be unavoidable if the Commission adopted broad classifications for parts of concern, and left it to applicants to determine whether particular parts are covered. Instead, the Covered List should identify *specific parts identification numbers* that have been deemed a security risk.

Third, because the Covered List is intentionally limited to determinations made by the designated national security agencies, the FCC should extend SEA restrictions to components *only when national security agencies themselves* identify specific part numbers of logic-enabled or otherwise significant components as constituting an unacceptable security risk. Without this level of granularity, there is simply no way to ensure that the risks identified by national security experts are being addressed in a clear and consistent manner. Furthermore, the SEA does not direct the Commission to police "components," whether that is defined to mean "modules" or something more granular. To the extent that the Commission seeks to add particular "components" to the list of items prohibited by the Covered List, it would be expanding the scope of the list, contrary to the terms of the law.

C. Any Attestation Requirements Should Be Narrow, and Focus on Preventing Circumvention of the Rules that Will Prohibit Covered Equipment from Receiving Authorization.

The Commission's inquiry regarding the scope of potential attestation rules implicates many of the same issues noted above. In particular, attestation requirements that apply to

component parts would require the same kind of detailed supplier tracking that, for the reasons described in Section IV.A., would impose undue burdens and costs on supply chains.

If the Commission were to create any attestation requirements for components, these attestations should be as narrow as possible. Such attestations should be limited to preventing Covered List equipment from being improperly incorporated into other equipment and circumventing the Commission's rules. Appropriately targeted attestation requirements for components would better align with the newly adopted rule that Covered List entities must use the certification process rather than the Supplier's Declaration of Conformity ("SDoC") process.[22] That requirement is an anti-circumvention measure that allows the Commission to more directly oversee Covered List equipment to ensure that such equipment does not make its way into the U.S. market. Attestations for component parts should be similarly limited, and only used to prevent entities from incorporating Covered List equipment as a component part.

The Commission should also not impose a general obligation on applicants to ensure that devices do not contain modules or components from entities on the Covered List if those modules and components are not themselves on the Covered List. To the extent that *national security authorities* determine that particular equipment should be "covered," said equipment can and should be designated and added to the Covered List.

The Covered List should also clearly distinguish between (1) entities whose finished goods are prohibited and (2) entities whose components are prohibited. Where there is overlap—i.e., where there is an entity whose finished goods *and* components are prohibited—the Covered List should make that clear as well. Regardless of any future additions, the

[22] FNPRM ¶¶ 75, 78-79.

Commission should avoid imposing attestation burdens on equipment for which no finding of national security risk has yet been made.

Finally, any attestation requirements should be limited to individual, specified parts. As explained, it is critical to uniformity of administration and risk mitigation that all entities understand which specific components pose a national security threat. The Covered List should only be expanded to list specific parts numbers and components on an individual basis, and any attestation requirements should closely track specific components designated on the Covered List.

D. Any Component Attestation Requirements Should Be Based on a Reasonable Investigation into the Supply Chain, and such an Investigation Should Permit—but Not Require—Applicants to Rely on Supplier Statements.

If the Commission creates component attestation requirements, it should only require companies to certify that the product for which they seek equipment authorization does not contain such covered components *based on a reasonable investigation* into whether their finished products use the components of a covered entity. Applicants seeking authorization should not be required to prove the negative, and a reasonable investigation into components should suffice for any attestation requirement.

As part of any reasonable investigation, the FCC should allow entities to rely on a supplier's compliance statements, but suppliers should not be required to obtain such statements. Reasonable investigations may involve relying on supplier statements, especially since some network providers may lack the ability to identify every component and its respective

manufacturer. NTCA's suggestion that network providers should be able to rely upon manufacturer certifications made to the Commission thus makes good sense.[23]

The Commission, however, should not turn NTCA's suggestions on this point into requirements. In the FNPRM, the Commission, drawing on NTCA's advocacy, sought comment on whether entities assembling end products should be *required* to obtain compliance statements from suppliers.[24] This approach is too prescriptive, lacks flexibility, and would be unduly burdensome, particularly if it goes beyond "covered" equipment itself and leads to speculative judgment calls about whether inclusion of a component in the device "could result in a device being classified as covered equipment[.]"[25] Ultimately, there is no way for a third party to know if a component "could result in a device being classified as covered equipment[.]"[26]

V. ANY REVOCATION OF EXISTING EQUIPMENT AUTHORIZATIONS WOULD CREATE SERIOUS COMPLICATIONS AND HARM CONSUMERS.

CTIA welcomes the Commission's focus on the concerns raised in the record to date about the problems and complications that would be caused by revoking existing equipment authorizations.[27] CTIA and others have already laid out many of these concerns in detail in the record, and nothing has changed to mitigate this issue.[28] These concerns remain significant, and the costs of revoking any equipment authorizations for devices that are in widespread consumer use are substantial. The Commission should also consider that revocations are likely to

[23] FNPRM ¶ 286 (The Commission states that these are NCTA's suggestions, but this suggestion comes from *NTCA*. *See* Comments of NTCA at 4).

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] *Id.* ¶¶ 290-91.

[28] *See, e.g.*, Comments of CTIA at 9-13; Comments of NCTA at 10-11; Comments of CTA at 14-16.

disproportionately impact low-income customers, the elderly, and disadvantaged groups, all of whom are less able to replace existing devices if existing equipment is barred. Such impacts further support the idea that any revocations must include a plan for government funding to replace devices and equipment.

A. Impact Assessments Should Be Required for Revocations, and Revocations Should Be Limited and Prospective.

As a general matter, the FCC should avoid revoking existing authorizations, and should do so only when it is specifically required by a finding of the relevant national security agency. Even then, implementation of a revocation that is called for by the national security agencies should be done in a manner that minimizes, as much as possible, the impact of that revocation on consumers and the surrounding marketplace. These determinations should consider the revocation's impact on consumers, communications networks, and the broader supply chain.

Revocations should generally be limited, prospective, and promote due process. As the FCC notes in the FNPRM, partial and limited revocation (i.e., by prohibiting future sale and import pursuant to existing authorizations of any devices after the date of the Interim Freeze Order) would reduce future risk while also minimizing the challenges associated with trying to remove existing devices from consumer hands.[29] Limited, forward-looking revocations would also avoid arguments about retroactive application. As a general rule, the Commission should favor such a limited and prospective approach, except in those extraordinary cases where the national security agencies specifically ask the Commission to retroactively revoke an authorization.

[29] *See* FNPRM ¶ 296.

Short of that, the Commission should only consider revoking equipment authorization if the equipment were found to violate the rules that were in place when it was initially approved or marketed. If the Commission were to retroactively revoke authorization based on a rule change, such that previously authorized products that would no longer be eligible for new authorizations must also have their prior authorizations withdrawn, it could invite arguments about whether other equipment authorization rule changes also would necessitate retroactive revocation. The Commission should avoid thorny questions raised by retroactive revocations.

B. Revocations Should Be Subject to Formal Hearing, Include a Phase-out Period, and Provide Guidance for Alerting Consumers.

If the Commission does revoke the authorization for existing devices, either because of a direction from the national security agencies or because of a lack of compliance with rules that existed at the time of approval or marketing, it should open a formal proceeding to conduct the revocation. This would provide due process to manufacturers and their customers, transparency to service providers and their customers regarding possible future revocations, and would ensure that the extremely complex issues associated with retroactive revocation are adequately considered by the agency.

In any revocation of authorizations for devices in the field, the FCC should also provide an adequate "runway" or phase-out period to allow those devices to be replaced.[30] These phase-out periods should be case specific, taking into account adequate time for replacement or substitution. These phase-out timeframes may differ, depending on the kind of device and the lifecycle of that device when purchased by a consumer or enterprise user. For example, infrastructure devices may require a longer phase-out runway than devices with faster turnover.

[30] *Id.* ¶ 297.

Regardless of the type of equipment, any process that the Commission develops to establish phase-out periods should consider stakeholder feedback.

Revocation should also only occur when the Commission is satisfied that adequate alternatives at affordable price points exist in the marketplace. The Commission should minimize harm to consumers and the supply chain as it works to mitigate threats identified by the national security agencies. The FCC should, at a minimum, ensure that there are sufficient market alternatives when considering whether to revoke authorization. Critically, any alternatives the Commission identifies should be similar in both function *and* cost.

The Commissions should ensure that revocations do not create additional policy problems, and it should specify that providers do not have the obligation to police the use of these devices on their networks. For example, the Commission should clarify that revocation does not impact devices being used in the United States by international roaming customers. The Commission should also ensure that providers will not face penalties for transmitting 911 calls placed from devices with revoked authorizations.[31]

Revocations should also in all cases be accompanied by agency guidance to make consumers aware of the revocation, advise them of how to proceed, and provide for the funding of replacements. The FCC should take on the task of conducting a public education campaign to make consumers aware of the revocation and advise them on how to proceed. The Commission, however, should not impose this obligation on network operators or other authorization holders. Revocation should include, for interested parties, explicit guidance explaining how to handle

[31] *See, e.g.*, 47 C.F.R. §§ 9.4, 9.10(b) (requiring carriers and CMRS providers to transmit all 911 calls to a public safety answering point ("PSAP"), a statewide default answering point, or to an appropriate local emergency authority).

revoked equipment. The Commission is in the best position to provide guidance for responses to revocations and can help coordinate industry's next steps.

Uncertainty and inconsistency would be particularly problematic if parties took differing approaches following a revocation, given the efforts that the industry and Commission have taken to empower consumers and encourage device portability.[32] Network operators should not be put in the position of guessing whether "covered" equipment should be allowed to operate on their networks, nor should they be required to police the use of "covered" equipment by their customers. In addition, if the FCC ultimately imposes obligations on carriers with respect to device revocation, it should equally impose such obligations on mobile virtual network operators ("MVNOs"), who are the entities in privity with affected customers. Lastly, consumers should be given clear information on why device bans are being imposed, and should not be confused about whether those bans originate with particular providers rather than by operation of FCC rules. Indeed, a lack of clarity on this last point could lead to differing approaches by providers, which could cause consumer confusion, competitive harm, and ultimately undermine national security objectives.

VI. THE COMMISSION SHOULD TAKE SUPPLY CHAIN AND CONSUMER HARMS INTO ACCOUNT WHEN CONSIDERING ANY ADDITIONS TO THE COVERED LIST.

The Covered List is intended to be able to evolve, with new entities and equipment added to the list when the relevant security agencies determine that statutory criteria are met. While the Commission does not have the discretion to modify these determinations, it does have the obligation to ensure that additions to the Covered List are implemented in a way that safeguards

[32] *See, e.g.*, *Cell Phone Unlocking*, FCC, https://www.fcc.gov/general/cell-phone-unlocking (last visited Mar. 30, 2023).

the public interest and are not unduly disruptive to or add unreasonable costs for consumers or industry.[33] As the FNPRM recognizes, now that adding equipment to the Covered List will bring consequences including authorization prohibitions and potential revocation, the Commission must consider how to mitigate harms that might arise from adding equipment to the Covered List.[34] These determinations should be made on a case-by-case basis.

While it may be the case that the addition of a piece of equipment is unlikely to cause significant disruptions, the Commission should be open to that possibility. For example, it would be very disruptive if a company that produces equipment for testing purposes were to be added to the Covered List. Testing equipment is vital to the smooth operation of the FCC certification process. Companies that perform testing for FCC certification are projected to have provided over 43,000 Form 731 application submissions projected in 2022,[35] and a delay of even a few months in the product approval plans could result in tens of thousands of products arriving late to market—or even potentially not coming to market. Any additions of equipment, like testing equipment, to the Covered List should allow users of such equipment adequate time to source and incorporate substitute equipment, a process that could take years. Further, should it go down this path, the FCC should develop reimbursement requirements for the replacement of such equipment.

---

[33] *See, e.g.*, 47 U.S.C. §§ 151, 201(b); *Telecommunications Carriers Eligible for Universal Service Support, Lifeline and Link Up Reform and Modernization*, Order on Reconsideration, 32 FCC Rcd 1095, ¶ 14 (2017) (explaining that consumer disruption can be contrary to the public interest and revoking Lifeline Broadband Provider designations on the basis of consumer disruption, among other reasons).

[34] *See* FNPRM ¶ 309.

[35] George Tannahill, Equipment Authorization System (EAS) Update, Laboratory Division Office of Engineering and Technology, FCC, at 4 (Apr. 27, 2022), https://transition.fcc.gov/oet/ea/presentations/files/apr22/13-Equipment-Authorization-System-Update.pdf.

VII. THE COMMISSION SHOULD AVOID POST-GRANT REVIEWS AND POST-MARKET SURVEILLANCE, WHICH WILL ONLY CREATE DELAYS AND FURTHER COSTS.

The Commission should not establish procedures that would allow review of post-grant equipment authorizations.[36] In the FNPRM, the Commission notes that comments in the record generally oppose the adoption of new procedures to allow public or government entities to weigh in, post-grant, to inform the Commission that particular equipment is in fact "covered" equipment.[37] As CTIA explained in its comments, any additional procedures would require additional resources and staffing; otherwise, long delays may result.[38] In addition, to the extent that there is doubt over whether particular equipment is "covered," it is the job of the security agencies to issue clarifications and amendments to the Covered List to remove such ambiguity.

The TCBs should also not be expected to conduct post-market surveillance on matters related to national security.[39] As CTIA laid out in its initial comments, charging TCBs with additional post-market surveillance to reach "covered" equipment status would increase costs and delays in application processing.[40] Post-market surveillance of "covered" status is fundamentally different from the kind of post-market surveillance that TCBs have generally been charged with conducting, such as ensuring that production devices conform to the technical specifications of the approval. TCBs have neither the experience nor the mandate to undertake these tasks. For example, TCBs simply are not equipped to conduct supply chain audits or track changes of control in equipment manufacturers to ensure that equipment does not become

[36] FNPRM ¶ 321.

[37] *Id.*

[38] Comments of CTIA at 19-20.

[39] FNPRM ¶ 322.

[40] Comments of CTIA at 19-20.

"covered" after an authorization is granted. Nothing in the record or in the Report and Order changes this commonsense conclusion.

The Commission should also take care to ensure enforcement of its new rules does not unduly impact or burden customers and other Commission stakeholders.[41] The Commission has adequate authority to enforce its new rules using the agency's customary processes. However, as with the implementation of the remainder of the rules, the Commission should ensure that actions taken to enforce the "covered" equipment restrictions do not unduly burden consumers or other industry stakeholders. This is particularly important when those consumers or stakeholders take steps in good faith to comply with the Commission's rules and guidance.

VIII. THE PROPOSED BIDDING CERTIFICATION SHOULD BE MORE TAILORED.

As the Commission suggests,[42] it would appear that any risks that might come from distortionary funding have decreased as a result of the various actions that the Commission has taken to implement the SNA and SEA. To the extent that authorization cannot be obtained for "covered" equipment, it is unclear what incentives would exist for entities to engage in distortionary funding beyond those that are covered by traditional investor analysis. Equipment manufacturers of "covered" equipment, for example, could no longer hope to benefit from providing assistance to particular bidders—even assuming this might have been a concern in the United States previously. Moreover, it is not clear what these certifications would accomplish in terms of solving actual problems that are not already covered by the Commission's rules, which require auction applicants to disclose all parties holding indirect ownership interest in the

[41] FNPRM ¶ 325.

[42] *Id.* ¶¶ 331-32.

applicant equaling 10 percent or greater.[43] As a result, if there ever was a need for additional bidding certifications, that need appears to have gone away.

If the Commission nevertheless proceeds with imposing certification requirements, any certification requirement adopted by the agency should be clear and understandable. Vague certification requirements in the context of spectrum auctions run the risk of making it harder to access capital in a timely way, decreasing the vibrant support that the Commission has seen for auctioned spectrum.[44] Certification requirements must also be consistent with already existing obligations.

As CTIA previously advocated, these goals would be met by a 10 percent threshold for disclosing "financial support" provided by parties that have been deemed to pose a national security threat under Section 54.9.[45] This remains especially true given the absence of any evidence that a lower threshold is needed to prevent a real, non-speculative potential harm. The Commission notes that CTIA did not provide a definition of "financial support" in its prior comments.[46] While CTIA does not have a specific definition in mind, any definition employed by the Commission should be clear and announced in advance, so that the market is clear on what kinds of financial arrangements are permissible. Ambiguous or uncertain rules—or rules whose application could potentially be sprung on bidders either during an auction or after bidding is complete—would have the inevitable effect of restricting access to capital, making it harder for prospective licensees to secure funding for auctions and reducing the overall.

[43] 47 C.F.R. §§ 1.2105(c)(5)(i), 1.2112(a)(6).

[44] *See* Comments of CTIA at 13-15.

[45] *Id.* at 14-15.

[46] FNPRM ¶ 330.

IX. 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. The Commission should encourage unified, risk-based policies that reflect ongoing and effective work in the private sector and at other agencies.

Respectfully submitted,

/s/ *Thomas C. Power*
Thomas C. Power
Senior Vice President, General Counsel

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

Justin Perkins
Manager, Cybersecurity and Policy

CTIA
1400 16th Street, NW, Suite 600
Washington, DC 20036
202-736-3200
www.ctia.org

April 7, 2023