Before the
Federal Communications Commission
Washington, D.C. 20554

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

Comments of the Telecommunications Industry Association

I. Introduction and Summary

The Telecommunications Industry Association ("TIA") appreciates the opportunity to provide additional input to the Federal Communications Commission ("FCC" or "Commission") on the above-captioned proceeding.[1] TIA was pleased to see broad consensus in initial comments responding to the FNPRM.[2] Consistent with TIA's initial comments, stakeholders across the information and communications technology ("ICT") sector agree that the Commission should not expend unnecessary time and resources to revoke existing equipment authorizations.[3] Nor should the Commission apply the Secure Equipment Act prohibitions expansively to components writ large.

[1] *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*, Report and Order, Order, and Further Notice of Proposed Rulemaking, ET Docket No. 21-232, EA Docket No. 21-233, FCC 22-84 (Nov. 11, 2022) ("FNPRM").

[2] We did note that several manufacturers on the Covered List filed comments objecting to various aspects of the Commission's proposals. Those arguments have been firmly rebutted in this and related records, and generally rejected by the Commission. There is no need to revive and rehear those arguments now. *See generally* Comments of Dahua Technology USA Inc., Hikvision USA, Inc., and ZTE Corporation, EA Docket No. 21-232 (filed Apr. 7, 2023).

[3] *See* Comments of Telecommunications Industry Association, EA Docket No. 21-232 (filed Apr. 7, 2023).

Instead, the Commission should take a targeted, risk-based approach to components that provides clear, workable guidance to manufacturers. Specifically, if the Commission extends equipment authorization prohibitions to components, it should (1) rely on national security agencies identified in the Secure Equipment Act to determine which specific components pose an unacceptable risk and explain why; (2) ensure that any rules prohibiting components limit burdens on consumers and manufacturers to the greatest extent possible; and (3) ensure that any attestation requirements rely on an applicant's reasonable investigation into the supply chain and likewise allow applicants to rely on the attestations of their suppliers. We elaborate on these themes below.

II. The Commission Should Not Revoke Existing Equipment Authorizations At This Time.

The record unequivocally reflects that the Commission should not revoke existing authorizations at this time. As numerous commenters note, any revocation of existing equipment authorizations would create serious complications and negatively impact consumers.[4] Moreover, no commenters suggest that revoking existing authorizations would have meaningful security benefits.[5]

Without new appropriations from Congress, such a revocation would engender an unfunded mandate with significant burdens on businesses and consumers. Such a revocation would perilously divert the resources of carriers and vendors from the nation's shared goal of

[4] *See* Comments of Consumer Technology Association, EA Docket No. 21-232, at 10-11 (filed Apr. 7, 2023) ("CTA"); Comments of CTIA, EA Docket No. 21-232, at 14-15 (filed Apr. 7, 2023) ("CTIA"); Comments of the Information Technology Industry Association, EA Docket No. 21-232, at 3-5 (filed Apr. 7, 2023) ("ITI"), Comments of USTelecom—The Broadband Association, EA Docket No. 21-232, at 5-8 (filed Apr. 7, 2023) ("USTelecom").

[5] We note Motorola urges the Commission to extend conditions and restrictions adopted in the Order to preclude marketing and sales of currently authorized "covered" equipment produced or provided by Hytera, Hikvision, and Dahua, but that the Commission can effectively tackle the national security threats posed by such equipment without deciding whether to revoke such authorizations. *See* Comments of Motorola Solutions, Inc., EA Docket No. 21-232, at 2 (filed Apr. 7, 2023).

expanding broadband to unserved communities and increasing capacity for growing connectivity demands. The ICT industry already faces a significant workforce shortage, which is even more acute in rural areas as the National Telecommunications and Information Administration ("NTIA") noted last year.[6] Moreover, as the Commission has observed in the context of the Secure and Trusted Communications Networks Reimbursement Program, removing revoked equipment would likely take several years. As the typical lifespan for equipment implicated in the Secure Equipment Act is limited (perhaps to as little as three to five years according to some estimates), any questionable equipment still in the market may be phased out anyway in the same amount of time. With this in mind, TIA sees no compelling reason for the Commission to revoke existing authorizations based on the current Covered List.

We agree with CTA and USTelecom that any future decision to revoke existing authorizations should be based on careful, thorough analysis of whether revocation is necessary to safeguard national security and if the security benefit of revocation outweighs other factors, including harm to consumers, cost and feasibility of compliance, and countervailing security risks.[7] If at some point in the future, the Commission finds that the benefit of removing covered equipment already in the marketplace outweighs the expense and harm imposed by requiring removal of that equipment, it should only do so when necessary funds have been appropriated to cover removal and replacement expenses.[8] We agree that in such a circumstance, the Commission should provide guidance to consumers and an appropriate transition period to

[6] NTIA, "Supply Chain & Workforce Development: In Preparation for IIJA Broadband Programs," at 13-14, (May 2022), Supply Chain Workforce Development Webinar_FINAL.pdf (doc.gov).
[7] *See* CTA at 11; USTelecom at 3.
[8] *See* CTIA at 6, Comments of NTCA—The Rural Broadband Association, EA Docket No. 21-232, at 4-5, (filed Apr. 7, 2023), USTelecom at 3.

minimize supply chain disruption and afford companies time to source, vet, and integrate alternative equipment.[9]

III. The Commission Should Take a Targeted, Risk-Based Approach to Components with Clear, Workable Guidance for Compliance.

The Commission should take a targeted, risk-based approach in considering whether and how to extend the Covered List prohibition to components. As commenters note, the ICT ecosystem is diverse, complex, and global. Any Covered List prohibitions applied to the components of a product for which FCC equipment authorization is sought will impose a significant burden on manufacturers and add complexity to the equipment authorization process.[10] Numerous commenters note challenges regarding the availability of certain components, particularly at a time when demand is high.[11] As such, if the Commission extends Covered List prohibitions to components, it should (1) rely on national security agencies to specify components that pose significant national security risk and provide clear reasoning as to why such components are considered a national security risk, (2) craft rules to reduce burdens on consumers and manufacturers, and (3) base attestation requirements on a reasonable investigation into the supply chain.

a. The Commission Should Rely on Determinations By National Security Agencies to Identify Specific Components Subject to the Prohibition.

If the Commission extends Covered List prohibitions to components, it should specify which components are subject to the prohibition based on determinations made by national security agencies that such components pose a significant national security risk. The Commission must clearly communicate to manufacturers which components fall within the

[9] *See* CTA at 11-12, CTIA at 6, ITI at 4, USTelecom at 3.
[10] *See* CTA at 7-10.
[11] *See* ITI at 5, USTelecom at 3-4.

scope of the prohibition in order for manufacturers to effectively comply with the rule.[12] Commenters agree that national security agencies must make such determinations to ensure that the national security risks addressed by the Covered List are handled in a clear and consistent manner.[13] The Commission should avoid developing its own standard, which may conflict with related approaches by the national security agencies and industry-led standards that may create a moving target that makes compliance more burdensome and expensive.[14]

b. The Commission Should Ensure That Any Rules Prohibiting Components Limit Burdens on Consumers and Manufacturers to the Greatest Extent Possible.

Recognizing that any rules extended to components will increase burdens on the ICT ecosystem, if the Commission extends the Covered List prohibition to components, it should draft rules to limit the impact on consumers and manufacturers as much as possible.[15] For example, the Commission should provide clear guidance to equipment authorization applicants and ample time for manufacturers to source, test, and integrate new parts into their products.[16] As commenters note, avoiding overly burdensome rules will enable more rapid and widespread compliance.[17]

c. Any Attestation Requirements Should Rely on an Applicant's Reasonable Investigation Into the Supply Chain and Allow Applicants to Rely on the Attestations of Their Suppliers.

If the Commission requires equipment authorization applicants to make attestations regarding components, such attestations should be based on the applicant's reasonable investigation into whether their finished product contains covered equipment. Commenters

[12] *See* CTA at 10, CTIA at 11, ITI at 7.
[13] *See* CTIA at 11, ITI at 6-7.
[14] *See* CTA at 8-9.
[15] *See id.* at 10.
[16] *See* CTIA at 11.
[17] *Id.* at 10.

agree that applicants cannot feasibly be required to "prove the negative" that their products contain no component from an entity on the Covered List.[18] Furthermore, companies must be allowed to rely on the statements and attestations of their suppliers that the products they source do not contain covered equipment.[19]

IV. Conclusion

TIA appreciates the Commission's crucial role in protecting the nation's communications networks from suppliers that pose a threat to national security and public safety. At this juncture, these goals are best served by a forward-looking focus on trusted networks. Based on the totality of the record, revoking existing authorizations at this time would not yield enough security dividends to outweigh the extreme costs that such an action would impose. Similarly, the Commission should only selectively apply the Secure Equipment Act prohibitions to components based on clear and compelling determinations made by national security agencies identified in the statute. At every stage, the Commission should endeavor to make this process as clear and workable as possible for trusted manufacturers working in good faith to comply with these new rules and simultaneously meet the growing connectivity needs of the American people. TIA and its members value the Commission's ongoing partnership in this effort and remain committed to ensuring that Americans benefit from a robust, trustworthy ICT supply chain.

_/s/_____
Colin Black Andrews
Senior Director, Government Affairs

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

May 8, 2023

[18] *See id.* at 13, ITI at 7.
[19] *See* CTIA at 13-14.