

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

In the Matter of	)	
	)	
Protecting Against National Security Threats to	)	ET Doc. No. 21-232
The Communications Supply Chain through the	)	
Equipment Authorization Program	)	

**Reply Comments of the
Telecommunications Industry Association**

Colin Black Andrews
Senior Director, Government Affairs

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1201 Wilson Boulevard, Floor 9
Arlington, VA 22209

September 28, 2026

Table of Contents

I.	Introduction and Summary	1
II.	Commenters Overwhelmingly Agree that Covered List Implementation Must Directly Reflect Underlying National Security Determinations and that Existing Flexibility in the Equipment Authorization Program Critically Enables U.S. Technology Leadership.....	3
III.	Challenges and Costs Associated with SBOM and HBOM Requirements Caution Against Adopting Such Mandates in the Equipment Authorization Program at This Time.....	6
	a. <i>Product Manufacturers Broadly Emphasize the Significant Challenges and Costs Associated with SBOMs and HBOMs.</i>	<i>7</i>
	b. <i>The FCC Can Enforce Covered List Rules Effectively Without SBOM and HBOM Mandates</i>	<i>10</i>
	c. <i>If the FCC Decides to Require SBOMs and HBOMs, It Should Take Steps to Reduce Security Risks and Minimize Burdens on Trusted Suppliers.....</i>	<i>12</i>
IV.	Conclusion	14

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

In the Matter of	)	
	)	
Protecting Against National Security Threats to	)	ET Doc. No. 21-232
The Communications Supply Chain through the	)	
Equipment Authorization Program	)	

**REPLY COMMENTS OF THE
TELECOMMUNICATIONS INDUSTRY ASSOCIATION**

I. Introduction and Summary

The Telecommunications Industry Association (“TIA”) appreciates the opportunity to respond to comments on the Third Further Notice of Proposed Rulemaking (“FNPRM”) issued by the Federal Communications Commission (“Commission” or “FCC”) in the above-captioned proceeding.¹ The initial comment round garnered substantial input from stakeholders across the information and communications technology (“ICT”) marketplace, including from numerous sectors that do not regularly engage with the Commission.

The resulting record reflects broad agreement on a number of important principles. Stakeholders overwhelmingly support the Commission's mission to protect U.S. communications networks from threats posed by foreign adversary suppliers and support effective implementation of both the Secure and Trusted Communications Networks Act ("Secure Networks Act") and Secure Equipment Act. At the same time, commenters consistently express concern that certain

¹ *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program*, Third Report & Order, Third Further Notice of Proposed Rulemaking, ET Doc. No. 21-232 (Jul. 22, 2026) (“Report and Order” or “FNPRM”).

proposals in the Third FNPRM, particularly those arising from recent production location-based Covered List determinations on certain identified device sectors, could impose significant costs and operational burdens without corresponding security benefits.

As discussed throughout these Reply Comments, the record supports the Commission's proposal to bifurcate the Covered List, codify rules that continue support for previously authorized equipment in the public interest, and adopt clear definitions that facilitate compliance while preserving beneficial commercial practices. Commenters were aligned that Covered List implementation must remain firmly rooted in the underlying national-security determinations that gave rise to a listing. Likewise, stakeholders broadly support preserving the flexibility necessary for innovation and product development within the equipment authorization program while focusing Commission resources on enhanced compliance tools and enforcement against bad actors. The record further reflects a consistent view that any new requirements should provide security benefits that outweigh their administrative burdens and should be accompanied by sufficient implementation periods to avoid unnecessary disruption and cost.

Although some customers, think tanks, and purveyors of security services tout the benefits of software and hardware bills of materials ("SBOM" and "HBOM," respectively), technology providers across the board identify major challenges to ubiquitous implementation and disclosure at this stage. As many commenters explain, the Commission does not require SBOM or HBOM mandates to enforce Covered List prohibitions effectively, and mandatory disclosure could in some circumstances undermine, rather than advance, national security objectives. The Commission can instead continue relying on established compliance mechanisms, including attestations, to hold authorization holders accountable, while working

with Telecommunications Certification Bodies ("TCBs") and stakeholders to evolve supporting documentation and guidance as standards and industry practices mature.

Accordingly, TIA urges the Commission to refrain from adopting SBOM or HBOM requirements as part of the equipment authorization process based on the overwhelming record in this docket. If the Commission ultimately determines that some form of disclosure obligation is necessary, it should consider targeting this requirement narrowly for sectors that are most relevant to achieving stated security goals and should take steps to minimize administrative burdens, protect sensitive commercial and security information, provide automatic levels of confidential treatment, and provide clear, practical guidance that regulated entities can realistically implement.

II. Commenters Overwhelmingly Agree that Covered List Implementation Must Directly Reflect Underlying National Security Determinations and that Existing Flexibility in the Equipment Authorization Program Critically Enables U.S. Technology Leadership.

Stakeholders across the ICT ecosystem overwhelmingly agree that effective implementation of the Secure Networks Act and Secure Equipment Act requires both targeted national security protections and continued flexibility within the equipment authorization program to support innovation, investment, and technology leadership. Indeed, commenters from across the communications, consumer technology, manufacturing, and broadband sectors recognize that national security and innovation are not competing objectives.² Rather, maintaining U.S. leadership in strategic technologies such as 6G, artificial intelligence, cloud services, advanced computing, connected devices, and secure communications infrastructure

² See e.g. Comments of Consumer Technology Association ("CTA"); Comments of CTIA; Comments of the Information Technology Industry Council.

requires a regulatory framework that appropriately addresses identified risks without imposing unnecessary barriers to development, deployment, and commercialization.³

This perspective is consistent with recent Administration policy emphasizing that efforts to protect sensitive science and technology must not unnecessarily impede innovation or private sector participation in national security objectives. As both policymakers and commenters have recognized, excessive regulatory burdens can undermine the very technological leadership and supply chain resiliency that national security policies seek to protect. Continued U.S. leadership in emerging technologies increasingly depends on our trusted allies, and the ability of trusted manufacturers, vendors, and suppliers to operate efficiently across global markets and supply chains.⁴

Commenters likewise recognize that the same manufacturers and suppliers responsible for advancing U.S. leadership in AI infrastructure, 6G deployment, advanced computing, cloud services, and secure communications technologies are often the entities that would bear the costs of significant new compliance obligations. As a result, the Commission should carefully assess whether additional requirements materially improve national security or simply divert resources away from innovation, network deployment, domestic manufacturing efforts, and supply chain

³ CTA Comments at 6; CTIA Comments at 5.

⁴ See, e.g., National Security Science & Technology Strategy, The White House, at 2-3 (Aug. 2026), <https://www.whitehouse.gov/wp-content/uploads/2026/08/NSSTS-082026.pdf> (recognizing that (i) “[e]fforts to protect sensitive S&T must protect Americans’ rights and liberties without unduly slowing the pace of innovation;” (ii) “[e]xcessive regulation and inefficient legacy policies must be changed or eliminated so that they do not inhibit the ability of American industry to contribute to national security needs;” and (iii) “[t]he Federal Government must partner effectively with the private sector, recognizing that the private sector contributes critical capabilities that the government does not possess.”); Remarks of Paul Dabbar, Deputy Sec’y, Com. Dep’t, “Launching the International Call to Action for 6G Leadership and Security,” at the Ctr. for Strategic & Int’l Stud. (July 29, 2026) (identifying “allied scale” as a core element of the Trump Administration’s 6G policy). See also Comments of CTA at 27-28; Comments of CTIA at 5-9.

diversification. With this in mind, the record supports the following actions in response to the Third FNPRM:

1. *Bifurcation*: Commenters support the Commission’s proposal to distinguish between producer/provider-based and production location-based categories, and acknowledge that the latter presents different security risks and implementation challenges and should therefore not automatically trigger the harsher restrictions developed for producer/provider-based determinations.⁵
2. *Allowance of Permissive Changes and Continued Equipment Support*: Commenters broadly support the codification of the Commission’s existing permissive change waivers to support continued reliability of previously authorized equipment and use the established process to restrict/ revoke authorizations only where absolutely necessary.⁶
3. *Definition of “Produced By”*: The record generally urges the Commission to adopt a definition of “produced by” that clarifies covered activities while preserving and clearly defining beneficial “white-labeling” commercial arrangements.⁷
4. *Component-Level Restrictions*: Commenters consistently urged the Commission to ensure that component-level restrictions directly reflect applicable national security determinations.⁸
5. *Flexibility Supports Innovation*: The record strongly supports preserving existing flexibility in the equipment authorization process, including the preservation of innovation pathways through use of Supplier’s Declaration of Conformity and existing exemptions for experimental and pre-authorization activities.⁹
6. *Targeted Enforcement and Compliance Modernization*: Stakeholders generally favor focusing enforcement efforts on bad actors while pursuing modernization of

⁵ See, e.g., Comments of CTA, CTIA, NEMA, Robostrategy, SEIA, TIA, USTelecom. While we recognize the FCC has no discretion regarding national security determinations provided by enumerated sources in the Secure Networks Act, TIA shares stakeholders’ concerns that recent production location-based national security determinations are not specific enough to fit the intention and use of Covered List authorities. See, e.g., Comments of CTA, CTIA, ITI. Bifurcating the Covered List rules to apply production location restrictions only to finished products identified in the underlying national security determinations is critical to reduce market disruptions and provide more clarity and certainty to the broad ecosystem of stakeholders reliant on these technologies.

⁶ See e.g., Comments of AUVSI, CTA, CTIA, ITI, NCTA, NEMA, NTCA, Robostrategy, SEIA, TIA, USTelecom. We encourage the FCC to codify these important allowances, including in cases where a U.S. part must be swapped for a part from a trusted manufacturer abroad.

⁷ See, e.g., Comments of AUVSI, CTA, CTIA, TIA, USTelecom.

⁸ See, e.g., Comments of AUVSI, CTA, CTIA, NEMA, NTCA, SEIA, TIA.

⁹ See, e.g., Comments of CTA, CTIA, NEMA, SEIA, TIA.

existing compliance systems and tools, such as the EAS Database, and ensuring that any newly adopted rules have a sufficient transition period.¹⁰

7. *Avoid Costly Requirements with no Tangible Security Benefit*: The record urged the Commission to avoid proposals like FCC logo requirements and authorization term limits that would impose more burdens and costs without a clear tie to a security concern or other similar compliance benefit.¹¹
8. *HBOM/SBOM and Software Provenance Requirements*: The record reflects substantial concerns regarding the feasibility, security implications, and cost of broad HBOM, SBOM, and software provenance mandates. Commenters generally support risk-based approaches that rely on supplier certifications, reasonable due diligence, audits, and targeted disclosures rather than universal reporting obligations.¹²

Overall, the record consistently urged the Commission to be mindful that the same manufacturers and suppliers responsible for advancing U.S. leadership in AI infrastructure, 6G, cloud services, advanced computing, and secure communications technologies are also the entities that would bear the cost of significant new compliance obligations. The Commission should remain mindful of the potential impacts on U.S. technological leadership and carefully assess whether additional requirements materially improve national security or merely divert resources from innovation, network deployment, and supply chain diversification.

III. Challenges and Costs Associated with SBOM and HBOM Requirements Caution Against Adopting Such Mandates in the Equipment Authorization Program at This Time.

TIA has long championed efforts to enhance ICT supply chain transparency and resiliency, including through development of its SCS 9001 supply chain security standard. However, the record in this proceeding confirms that broad hardware bill of materials ("HBOM") and software bill of materials ("SBOM") mandates are not the most effective way to achieve

¹⁰ See, e.g., Comments of CTA, TIA, USTelecom.

¹¹ See, e.g., Comments of AUVSI, CTA, CTIA, NEMA, TIA, USTelecom.

¹² See, e.g., Comments of CTA, CTIA, TIA, USTelecom.

those objectives. In fact, the lack of a common, automated reporting standard, combined with the highly sensitive nature of the information contained in HBOMs and SBOMs, raises significant concerns regarding the practicality, cost, and security implications of such requirements.

Fortunately, the Commission does not need to adopt HBOM or SBOM mandates to effectively enforce Covered List prohibitions. Existing mechanisms, including equipment authorization attestations and the Commission's existing enforcement authorities, already provide a workable framework for ensuring compliance while avoiding the substantial burdens associated with a new supply chain reporting regime. The Commission can also continuously monitor and update guidance to TCBs as existing standards and practices evolve to keep the Commission's guidance current. If the Commission ultimately determines that additional HBOM and SBOM mandates are necessary, it should take steps to minimize any additional administrative burdens, devote significant resources to protecting this sensitive information, ensure such information receives automatic levels of confidential treatment, take efforts to harmonize new rules with global SBOM requirements, and provide industry with clear and workable compliance guidance.

a. Product Manufacturers Broadly Emphasize the Significant Challenges and Costs Associated with SBOMs and HBOMs.

In the record of this proceeding, stakeholders across the ICT industry emphasize critical challenges associated with SBOMs and HBOMs.¹³ As many commenters note, developing and maintaining uniform SBOMs and HBOMs would impose substantial administrative and

¹³ See, e.g., Comments of CTA, CTIA, NEMA, TIA, USTelecom.

operational burdens on equipment authorization participants, creating meaningful concerns for large global suppliers and potentially prohibitive costs for smaller entities.¹⁴

These concerns are amplified by the realities of modern technology supply chains. As agencies have recognized in related proceedings, software and hardware supply chains are necessarily global, highly dynamic, and increasingly complex.¹⁵ Components, suppliers, and sourcing arrangements routinely change to address capacity constraints, allocation issues, end-of-life products, quality improvements, and shifting market conditions. Given these dynamic and shifting supply chains, once an HBOM or SBOM has been compiled, it can quickly become outdated as upstream suppliers make substitutions in response to changing conditions.

Indeed, as the Commission is already aware from recent permissive change waiver requests, manufacturers currently operate in an environment characterized by component shortages, surging demand driven by emerging technologies, and an increasingly complex global regulatory landscape.¹⁶ Further, introducing a new burden via a filing requirement for an updated BOM each time a component or country of origin changes could actually run afoul of the Commission's intended goals. Such a requirement would likely reduce supply chain resiliency by discouraging beneficial substitutions, instead increasing the reliance on a limited

¹⁴ See, e.g., Comments of CTA.

¹⁵ This is one reason the Department of Commerce, for example, opted not to impose SBOM/HBOM requirements in the Connected Vehicles Final Rule. See Bureau of Industry & Security, U.S. Dep't of Com., Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles, 90 Fed. Reg. 5360, 5496-5398 (Jan. 16, 2025) (BIS recognized concerns that proposed HBOM and SBOM requirements were "overly burdensome" and would require regulated entities to "devote substantial resources to meet compliance," and therefore rejected the proposal to submit SBOMs and HBOMs with Declarations of Conformity).

¹⁶ See, e.g., NCTA Waiver Request, <https://www.ntca.org/sites/default/files/federal-filing/2026-06/ntca-aca-petition-%20waiver-6262026.pdf>.

number of suppliers within specific component markets in order to mitigate the cost of compliance with the FCC's requirements.

Similarly, as we raised in our initial comments and others raised on the record, software supply chains present their own challenges.¹⁷ Modern software products often rely on open-source components, third-party libraries, and dependencies over which downstream suppliers have only limited visibility. Establishing and maintaining accurate SBOMs and HBOMs would therefore require significant ongoing investments to collect information from suppliers and sub-tier suppliers, conduct engineering reviews and validation, perform legal and regulatory assessments, and continually update disclosures throughout a product's lifecycle. These substantial capex and opex costs would inevitably be passed on to consumers.

Commenters also highlight the significant security, competition, and innovation risks associated with mandatory disclosure of SBOMs and HBOMs.¹⁸ Such materials may reveal highly sensitive commercial information, including production architectures, component-selection strategies, supplier relationships, software dependencies, security implementations, manufacturing practices, and proprietary research and development investments. Disclosure of this information, even to the government, carries inherent risks of unauthorized access, misuse, or inadvertent release. Moreover, concentrating large quantities of sensitive technical and commercial information within a single repository could create additional cybersecurity concerns and increase the attractiveness of that repository as a target for malicious actors. This is particularly concerning with respect to foreign adversaries, who might view the FCC as a more

¹⁷ See e.g. TIA Comments.

¹⁸ See e.g. Comments of CTA at 28-32; Comments of CTIA at 18-22; Comments of ITI at 7; Comments of the National Electrical Manufacturers Association at 2.

attractive target for cyber campaigns if quantities of sensitive technology and commercial information are stored there.

Finally, it is worth cautioning that detailed BOM disclosures could provide valuable information to counterfeiters and other bad actors, which could itself increase, rather than reduce, the Commission's equipment-authorization enforcement costs and challenges.¹⁹

Taken together, the substantial costs, implementation challenges, and security risks identified throughout the record outweigh any incremental enforcement benefits the Commission might achieve through a broad SBOM or HBOM mandate.

b. The FCC Can Enforce Covered List Rules Effectively Without SBOM and HBOM Mandates.

Fortunately, the FCC does not need SBOM/HBOM mandates to effectively enforce the Covered List rules. As commenters note, existing mechanisms already require equipment authorization applicants to conduct ongoing supply chain diligence and certify that their products comply with Covered List restrictions. These attestation requirements enable the Commission to hold authorization holders accountable for their representations while ensuring that Covered List prohibitions remain fully enforceable.²⁰

TIA also recognizes the concerns raised by downstream providers who correctly emphasize that they should not be held responsible and even liable for supply chain information that they have no practical ability to access, verify, or control.²¹ In many cases, manufacturers,

¹⁹ TIA members note that the FCC currently requires filing of internal photos, parts lists, and device schematics, sensitive data which could enable bad actors and counterfeiters at a significant cost to OEMs.

²⁰ See, e.g., Comments of CTA, TIA.

²¹ See, e.g., Comments of NCTA, NTCA.

service providers, and integrators necessarily rely on representations from suppliers regarding the origin and composition of components incorporated into their products. With that in mind, TIA agrees that the FCC should permit such entities to rely on representations of their suppliers and publicly available information, including information provided by the FCC itself, based on a reasonable investigation into that entity's supply chains. The Commission could further support compliance efforts by directing the Office of Engineering and Technology to work with stakeholders to develop guidance regarding what constitutes a reasonable investigation, particularly for smaller entities with more limited compliance resources.

To be sure, several think tanks, certification providers, and security-focused organizations identify theoretical transparency benefits associated with SBOM and HBOM requirements.²² Notably, these comments did not come from manufacturers themselves with the requisite knowledge of how complex, global ICT supply chains operate, and with familiarity of the complexities involved in obtaining regulatory authorization for launching a new device. Further, these commenters generally do not demonstrate how such theoretical benefits would outweigh the substantial implementation challenges, administrative burdens, costs, and security risks identified throughout the record. Nor do they explain why existing attestation and enforcement mechanisms are insufficient to ensure compliance with Covered List restrictions.

Accordingly, the record demonstrates that the Commission can continue enforcing Covered List prohibitions effectively without transforming the equipment authorization process into a broad supply-chain reporting regime. The Commission's existing tools, through

²² See, e.g., Comments of FDD, Gatewell, iCertifi, Modgud, PolkaSpots.

attestations and a flexible compliance framework, are more than sufficient for enforcing new rules regarding production location-based Covered List additions.

- c. If the FCC Decides to Require SBOMs and HBOMs, It Should Take Steps to Reduce Security Risks and Minimize Burdens on Trusted Suppliers.*

Although TIA believes the record counsels against adoption of broad SBOM and HBOM mandates at this time, the comments nonetheless provide useful guidance should the Commission determine that some form of disclosure requirement is necessary. If the FCC ultimately proceeds, it should adopt safeguards that minimize security risks, reduce unnecessary administrative burdens, and provide regulated entities with a clear and workable compliance framework. At a minimum, the Commission should:

1. *Ensure that SBOMs and HBOMS Can Be Requested Rather than Mandated as Part of the Authorization Process:* Consistent with the Commission's other cybersecurity and supply chain rules, the FCC should not require routine submission of SBOMs and HBOMs as part of every equipment authorization application. Instead, authorization holders should be required to provide such information upon request during an investigation or other compliance review. This approach would preserve the Commission's ability to obtain relevant information when necessary while significantly reducing the risks and administrative burdens associated with maintaining large volumes of sensitive supply chain data.²³
2. *Take Steps to Limit the Scope and Impact on Regulated Entities:* If the Commission proceeds with some form of a mandatory BOM submission requirement, it should narrowly target the scope of such a mandate to only impact sectors that are specifically related to a national security interest, rather than the ICT sector at large, and the Commission should harmonize BOM requirements with existing international device requirements to avoid duplication for global entities.
3. *Provide Clear Guidance and Limit Required Disclosures:* The Commission should provide clear guidance regarding the structure and substance of HBOMs/SBOMs and limit disclosure to first-tier components and country-of-origin only for components on the Covered List. This narrowly tailored approach

²³ See, e.g., Comments of CTA, TIA.

would improve consistency across filings while reducing unnecessary compliance costs.²⁴

4. *Limit Disclosure of Proprietary Information:* As numerous commenters note, SBOMs and HBOMs may include proprietary, highly sensitive commercial, technical, and operational information.²⁵ The Commission should avoid mandating the inclusion of such proprietary supply chain information as that does not directly relate to the FCC's national security objectives.
5. *Permit Reasonable Due Diligence and Avoid Duplication:* The Commission should permit applicants to meet any reporting obligations through reasonable supply chain diligence and by leveraging existing compliance frameworks wherever possible. The FCC should avoid creating duplicative reporting requirements that force manufacturers to develop entirely new compliance systems solely for this proceeding.²⁶
6. *Adopt a Materiality Threshold for Reporting and Update Existing Databases:* Rather than requiring updates within a fixed period following every change, the Commission should establish a materiality threshold for reportable modifications. The FCC should also ensure that its databases, submission portals, and information-security practices can receive, store, and appropriately process sensitive supply chain information before imposing any new reporting requirements, and any information submitted to the FCC should be automatically treated as confidential.²⁷
7. *Define Third Party Responsibilities:* The Commission should reduce ambiguity by clearly defining the responsibility of licensors, suppliers, manufacturers, integrators, and other third parties.²⁸
8. *Establish a Reasonable Transition Period:* If adopted, any HBOM or SBOM requirements should be accompanied by a meaningful transition period that allows equipment authorization participants to develop compliance programs, coordinate with suppliers, establish reporting processes, and implement necessary technical and operational changes. The record consistently reflects that compliance would require substantial planning and investment.²⁹
9. *Establish a Good-Faith Safe Harbor:* Finally, the Commission should establish a safe harbor for authorization holders acting in good faith and relying on

²⁴ See, e.g., Comments of AUVSI, CTA, Robostrategy, SEIA.

²⁵ See, e.g., Comments of Commercial Drone Alliance, CTA, Robostrategy, SEIA, TIA.

²⁶ See, e.g., Comments of AHAM, Carnegie Endowment for International Peace, CTA, SEIA, TIA.

²⁷ See, e.g., Comments of AHAM, Commercial Drone Alliance, CTA, SEIA, TIA.

²⁸ See, e.g., Comments of CTA, TIA.

²⁹ See, e.g., Comments of AUVSI, CCIA, Commercial Drone Alliance, CTA, ITI, NEMA, TIA.

reasonable supplier representations. Regulated entities should not face enforcement exposure for information beyond their reasonable ability to verify, particularly where they have conducted appropriate diligence and complied with Commission guidance. Such a safeguard would encourage compliance while recognizing the practical limits of visibility into increasingly complex, global supply chains.

IV. Conclusion

TIA appreciates the Commission's continued efforts to protect U.S. communications networks from threats posed by foreign adversaries while ensuring the Covered List remains an effective tool for implementing the Secure Networks Act and Secure Equipment Act. As the record in this proceeding demonstrates, stakeholders across the ICT ecosystem broadly support the Commission's efforts to ensure U.S. networks are supported by trusted equipment, and that consumers have access to trusted, innovative ICT products and services. Proposals in the FNPRM to distinguish between producer/provider-based and production location-based Covered List determinations, preserve support for previously authorized equipment, maintain flexibility for innovation and product development, and focus enforcement efforts on bad actors and modernized compliance tools, rather than broad new administrative burdens, all effectively serve this goal.

By contrast, while supply chain transparency remains an important objective, broad SBOM and HBOM mandates are neither necessary nor practical to effectively enforce Covered List restrictions at this time and could undermine U.S. competitiveness and the very national security goals the Commission seeks to address. Accordingly, TIA urges the Commission to refrain from adopting any SBOM or HBOM mandates. TIA looks forward to continuing to work with the Commission to strengthen U.S. networks, promote trusted communications

infrastructure, and ensure that the equipment authorization program remains efficient, predictable, and supportive of continued U.S. technology leadership.

/s/
Colin Black Andrews
Senior Director, Government Affairs

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1201 Wilson Boulevard, Floor 9
Arlington, VA 22209

September 28, 2026