

**Before the
Federal Communications Commission
Washington, DC 20554**

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

**REPLY COMMENTS OF
NTCA–THE RURAL BROADBAND ASSOCIATION**

NTCA–The Rural Broadband Association (“NTCA”)¹ hereby submits these reply comments in the above-referenced proceeding.² While recognizing and supporting generally the Commission’s efforts to secure communications networks, the record underscores the Commission’s lack of authority to undertake the specific actions proposed in the *Notice*. Commenters further demonstrated the impossible task of identifying and locating every piece of equipment that the Commission deems a threat to national security, and pulling such equipment

¹ NTCA represents approximately 850 independent, community-based companies and cooperatives that provide advanced communications services in rural America and more than 400 other firms that support or are themselves engaged in the provision of such services.

² *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program*, Notice of Proposed Rulemaking and Notice of Inquiry, ET Docket Nos. 21-232 *et al* (June 17, 2021), 86 FR 46641 (July 28, 2021) (“*Notice*”).

out of service, if the Commission should opt to retroactively revoke any equipment authorization as proposed in the NOI.

The *Notice* proposes using the equipment authorization process to block equipment the Commission has deemed a threat to national security and has published on the Covered List.³ The Commission cited as potential bases for this authority the equipment authorization rules, the Secure Networks Act or the Communications Assistance for Law Enforcement Act (“CALEA”).⁴ The Commission also referred to “broad authority” under the Communications Act to adopt rules as a basis for the rules proposed in the *Notice*.⁵ Commenters consistently demonstrated that none of these forms a basis for use of the equipment authorization process to exclude equipment on the Covered List.⁶ As CTIA pointed out, citing to a D.C. Circuit court opinion, “[t]he FCC cannot act in the ‘public interest’ if the agency does not otherwise have the authority to promulgate the regulations at issue....”⁷ In other words, regardless of the justification for action being considered, there must first be statutory authority for the Commission to act. In the present instance, however, there is no statutory authority for the rules proposed by the Commission.

Even those who asserted that the Commission should adopt the proposed rules failed to provide any existing legal basis for such action. The Coalition for a Prosperous America, for

³ *Notice* at ¶ 47.

⁴ *Notice* at ¶¶ 65-69.

⁵ *Notice* at ¶ 65.

⁶ *See, e.g.*, Comments of NCTA – The Internet and Television Ass’n, ET Docket No. 21-232 *et al* (Sep. 20, 2021) at pp. 2-3 (“NCTA Comments”); Comments of ACT – The App Ass’n, ET Dockets No. 21-232 and 21-233 (Sep. 20, 2021) at p. 2; Comments of the Information Technology Industry Council, ET Docket No. 21-232 *et al* (Sep. 20, 2021) at p. 14.

⁷ Comments of CTIA, ET Docket No. 21-232 *et al* (Sep. 20, 2021) at p. 36, citing *Motion Picture Ass’n of Am., Inc. v. FCC*, 309 F.3d 796, 806 (D.C. Cir. 2002) (“CTIA Comments”).

instance, cites important economic reasons for the Commission’s proposal but fails to identify any legal basis for the Commission to undertake the proposed actions.⁸ Likewise, the Telecommunications Industry Association asserted “the banning of all equipment from Covered Entities from U.S. networks, was a ‘logical outgrowth’ of all the work the [Commission] has been doing the past four years in the USF/Rip and Replace docket.”⁹ A “logical outgrowth,” however, does not provide the legal authority necessary to undertake actions not delegated to the Commission by Congress.¹⁰ TIA also suggests the Secure Equipment Act pending in Congress would provide authority to use the equipment authorization process to exclude equipment manufactured by companies on the Covered List.¹¹ Congress expresses its intention, however, by passing laws rather than considering bills.

Furthermore, as the Consumer Technology Association pointed out, the Commission has options already in place that can be used to advance the important objectives identified in the *Notice*, including partnering with NTIA and other federal agencies to share cybersecurity information that can be communicated to equipment manufacturers through the Communications Supply Chain Risk Information Partnership.¹² Similarly, the Commission could engage the Communications Security Reliability and Interoperability Council in identifying methods of

⁸ Comments of The Coalition for a Prosperous America, ET Docket No. 21-232 *et al* (Sep. 16, 2021).

⁹ Comments of the Telecommunications Industry Ass’n, ET Docket No. 21-232 *et al* (Sep. 20, 2021) at p. 5 (“TIA Comments”).

¹⁰ See NCTA Comments at p. 8, citing *Huawei Techs. USA, Inc. v. FCC*, 2 F.4th 421 (5th Cir. 2021).

¹¹ TIA Comments at pp. 6-7.

¹² Comments of the Consumer Technology Ass’n, ET Docket No. 21-232 *et al* (Sep. 20, 2021) at p. 13.

securing communications network equipment.¹³ These alternatives also offer the benefit of having the flexibility to adapt their inquiries and recommendations more readily according to ongoing, and changing, security concerns. This ability to adapt could result in more robust protections than could be obtained through Commission rules.¹⁴

Finally, NTCA encourages the Commission to coordinate with other federal agencies to avoid unintended consequences. For instance, the proposed rules as described in the *Notice* could prohibit the purchase of certain foreign equipment specifically allowed by the Department of Homeland Security.¹⁵ Similarly, the Commission’s proposed rules could conflict with international standards, thereby creating even more challenges to providers seeking to acquire the equipment and components necessary to maintain and expand their networks.¹⁶ Providers as well as equipment manufacturers need certainty that their purchases and operations, while permissible by one federal agency, are not then impermissible according to another agency.

Many commenters, like NTCA, support efforts to protect communications networks from harm and in fact are actively engaged in activities already underway with other federal agencies to do just that.¹⁷ The Commission likewise is engaged in many of these activities. To achieve

¹³ See, e.g., CTIA Comments at p. 31.

¹⁴ See, e.g., TIA Comments at p. 15 (“effective cybersecurity requires far more than the one-time testing against static technical criteria or check-the-box certifications that the FCC effectively and efficiently leverages in its equipment authorization regime.”); CTIA Comments at p. 30.

¹⁵ See Comments of PowerTrunk, Inc., ET Docket No. 21-232 *et al* (Sep. 20, 2021) at p. 2.

¹⁶ See, e.g., TIA Comments at p. 16. See also Comments of NTCA – The Rural Broadband Ass’n, ET Docket No. 21-232 *et al* (Sep. 20, 2021) at pp. 5-6.

¹⁷ NTCA is an active member of the Information and Communications Technology Supply Chain Risk Management Task Force, a public-private partnership with the Cybersecurity and Infrastructure Agency, the Communications Security, Reliability and Interoperability Council and the National Council of ISACs (Information Sharing and Analysis Center).

the objectives set forth in the *Notice*, NTCA encourages the Commission to continue engaging in these activities, with industry and other agencies, to provide timely responses and expertise.

Respectfully submitted,



By: /s/ Michael Romano

Michael Romano

Jill Canfield

Tamber Ray

4121 Wilson Boulevard

Suite 1000

Arlington, VA 22203

703-351-2000 (Tel)