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

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program Communications Sector | ) | 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**
**NTCA–THE RURAL BROADBAND ASSOCIATION**

NTCA–The Rural Broadband Association ("NTCA")[1] hereby submits these comments in response to the proposal by the Federal Communications Commission ("Commission") to revise the Commission's equipment authorization rules to prohibit any covered equipment on the list published by the Commission of equipment deemed a threat to national security ("Covered List").[2] NTCA supports efforts to enhance our nation's cybersecurity. In doing so, however, the Commission must ensure any equipment certifications fall within the appropriate Commission

[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 No. 21-232 *et al* (June 17, 2021), 86 FR 46641 (July 28, 2021) ("*Notice*").

authority, are narrowly tailored to prevent harm that would result from adding further delays to equipment availability and are not applied retroactively.

## I. THE PROPOSED RULES EXCEED THE COMMISSION'S EQUIPMENT AUTHORIZATION AUTHORITY AND WOULD DUPLICATE MEASURES ALREADY EMPLOYED BY OTHER AGENCIES.

The Commission proposes in the *Notice* to require applicants seeking equipment authorization to provide a written attestation stating that the equipment for which the applicant is seeking certification is not "covered" equipment on the Covered List.[3] The Commission further seeks comment on how the equipment authorization program could be used to "encourage manufacturers … to consider cybersecurity guidelines and procedures."[4] While NTCA supports efforts to protect the nation's telecommunications infrastructure from cyber threats, expanding the scope of the Commission's equipment authorization rules as a means of carrying out this goal exceeds the scope of the Commission's authority. Specifically, Section 302 of the Communications Act ("Act") grants the Commission authority to adopt regulations governing the interference potential of devices capable of emitting radio frequency ("RF") energy and that are capable of interfering with radio communications.[5] Part 2 of the Commission's rules codifies this section by establishing the equipment authorization procedures for RF devices only.[6]

[3] *Notice* at ¶ 47.

[4] *Notice* at ¶ 98.

[5] *See* 47 U.S.C. § 302(a).

[6] *See* 47 C.F.R. § 2.901. *See also Amendment of Parts 0, 1, 2, 15 and 18 of the Commission's Rules regarding Authorization of Radiofrequency Equipment*, Report and Order, ET Docket No. 15-170, 32 FCC Rcd 8746, 8747 (2017).

The Commission's proposal would also duplicate efforts already undertaken by other federal agencies to prompt equipment manufacturers to build more security into their products. The National Institute of Standards and Technology ("NIST"), for instance, has been collaborating with industry to develop technologies and standards to improve the security of Internet of Things ("IoT") devices. As part of this effort, NIST released a report in May 2021 on a Manufacturer Usage Description ("MUD") standard "to reduce both the vulnerability of IoT devices to network-based attacks and the potential for harm from any IoT devices that become compromised.[7] Likewise, the National Telecommunications and ("NTIA") has recently undertaken multiple cybersecurity efforts, including the development of a Software Bill of Materials, pursuant to an Executive Order, intended to "help create a more transparent and secure software supply chain."[8]

Instead of attempting to use existing equipment authorization rules for the certifications proposed in the *Notice* – an attempt that exceeds the clear scope of the Act – NTCA recommends the Commission coordinate IoT security with NIST, NTIA and other federal agencies undertaking cybersecurity efforts to ensure consistency and to offer additional expertise. Alternatively, or in addition to working with NIST to further ongoing security efforts, the Commission could ask Congress to amend the Secure and Trusted Communications Network Act

[7] NIST Special Publication 1800-15, Securing Small-Business and Home Internet of Things (IoT) Devices: Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD), May 2021, available at Securing Small-Business and Home Internet of Things (IoT) Devices: Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD) (nist.gov) (last visited Aug. 23, 2021) (With MUD, "the network will automatically permit the IoT device to send and receive only the traffic it requires to perform as intended, and the network will prohibit all other communication with the device, thereby increasing the device's resilience to network-based attacks.").

[8] NTIA Releases Minimum Elements for a Software Bill of Materials (July 12, 2021), available at https://ntia.gov/blog/2021/ntia-releases-minimum-elements-software-bill-materials (last visited Sep. 7, 2021).

of 2019 ("Secure Networks Act") to require manufacturers to certify that their equipment does not contain any covered equipment identified on the Covered List. NTCA also encourages the Commission not to duplicate efforts already undertaken by federal agencies whose primary mission is cybersecurity, including steps already taken steps by those agencies to better secure communications and IoT equipment from cyber attacks.

If the Commission concludes that subjecting all telecommunications equipment to the Commission's equipment authorization process is necessary to ensure covered equipment identified on the Covered List does not enter U.S. telecom networks, then providers should be able to rely upon any Commission equipment authorization going forward when certifying that they do not have any covered equipment in their networks. Presently, as NTCA has previously expressed to the Commission, network providers, especially small ones, have limited ability to identify the manufacturer of every component contained within any given piece of equipment and yet, these same providers are required to certify to the Commission that they do not have any covered equipment in their network.[9] Failure to meet this obligation comes with significant penalties.[10] Thus, at a minimum, providers should be able to rely upon any certifications made to the Commission by equipment manufacturers, regardless of the authority under which such certification is made.

[9] *See* NTCA Comments, WC Docket No. 18-89 (Feb. 3, '20), p. 7.

[10] *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Third Report and Order, WC Docket No. 18-89 (July 14, '21) at ¶ 38 (ETC recipients of USF support must certify that they have removed and replaced covered equipment from their networks as a condition to receiving USF support each year.). *See also* Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, Sec. 7(b) ("Secure Networks Act").

Furthermore, if the Commission chooses to use the equipment authorization process to prohibit covered equipment named on the Covered List, the Commission should be as clear as possible regarding the scope and limits of such bans. For example, the Covered List includes surveillance equipment manufactured by Hytera and Hikvision "to the extent it is used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, including telecommunications or video surveillance services provided by such entity or using such equipment."[11] The same surveillance equipment that is prohibited for use in the aforementioned circumstances is also used routinely by individuals and private businesses for personal security. As a practical matter, the equipment authorization process cannot identify how such equipment will be used. Accordingly, the Commission should use the instant proceeding to clarify how the Commission will apply the equipment authorization process to equipment that is "covered" based on certain uses while not "covered" for other uses.

## II. DELAYS IN THE AVAILABILITY OF COMMUNICATIONS EQUIPMENT RESULTING FROM THE TIME NEEDED FOR ALL COMMUNICATIONS EQUIPMENT TO PASS THROUGH THE COMMISSION'S EQUIPMENT AUTHORIZATION PROCESS WILL AFFECT PROVIDERS' ABILITY TO MEET APPLICABLE BUILDOUT DEADLINES.

The Commission's proposal in the instant proceeding significantly expands the number and types of equipment subject to the Commission's equipment authorization process. The time needed for manufacturers to make the required certification for all of their communications equipment and for the Commission to process the additional certifications will almost certainly result in a delay prior to such equipment being commercially available. Such a result would

[11] Public Safety and Homeland Security Bureau Announces Publication of the List of Equipment and Services Covered by Section 2 of the Secure Networks Act, WC Docket No. 18-89, Public Notice, 36 FCC Rcd 5534, 5536 (2021).

almost certainly exacerbate already increasing supply chain delays. Accordingly, the Commission would need to factor the added delay into buildout obligations under various Commission programs and should consider the implications for comparable deadlines under programs overseen by other federal agencies or States.

As NTCA noted in comments earlier this year, the equipment delays experienced by providers began a year or more ago and extend to communications equipment of all kinds, including electronics such as routers, optical network terminals, and customer premises equipment.[12] Providers are not only continuing to experience these delays but, in some instances, the delays are getting longer - extending over a year in some cases. These increasing delays, combined with uncertain equipment availability dates, are causing providers to work hard to find enough equipment to complete existing projects while, in some instances, being forced to place a hold on future buildout plans. Furthermore, providers who must remove and replace Huawei and ZTE equipment from their networks are faced with securing equipment at nearly the same time and from only a few vendors – an effort that is compounded by existing equipment delays.[13] The Commission therefore should not and cannot consider the actions here in a vacuum but rather, should fully consider the implications of the instant proposals on the Commission's own broadband deployment objectives and those of other governmental entities in crafting any new rules.

---

[12] *See* NTCA Comments, WT Docket 21-195 (June 10, 2021), p. 2. One NTCA member also reported experiencing a delay and shortage in the delivery of trucks, which are needed to complete repairs and installations.

[13] *See, e.g.*, Letter from USTelecom to Marlene H. Dortch, WC Docket 18-89 (July 7, 2021), p. 2 ("there will be extremely large demand for replacement communications equipment from a limited number of vendors due to the program….").

## III. THE COMMISSION SHOULD NOT APPLY ANY EQUIPMENT CERTIFICATION REQUIREMENTS RETROACTIVELY.

The Commission has also sought comment on whether to apply the equipment authorization process retroactively to equipment already deployed in providers' networks. Applying any equipment authorization or certification requirement retroactively would be highly detrimental to providers that relied in good faith upon the Commission's rules as they stood at the time such equipment was procured. Indeed, the Commission itself has recognized the harmfulness of requiring providers to replace covered equipment retroactively as well as Congress' intention that providers "rip and replace" covered equipment *after* Congress has allocated funding necessary to reimburse affected providers.[14]

Applying any prohibition retroactively, even with federal reimbursement for the cost of removing and replacing affected equipment, would be harmful to providers and result in even further equipment delays due to providers' need to purchase equipment necessary to replace equipment already in their networks in addition to equipment necessary to expand their service to new areas. This would likely impact small providers even more significantly due to the limited number of employees at most small providers, thereby forcing those providers to redirect their staff from expanding the providers' network availability to identifying suitable replacement equipment that, at least at the time of acquiring such equipment is not prohibited by the Commission, removing existing equipment, and then installing and testing the new equipment.

[14] *See Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Third Report and Order (July 14, 2021) at ¶ 34 ("We believe that Congress intended to make reimbursement funds available for all such equipment and services participants are required to remove.").

Such an outcome is directly contrary to the Commission's and Congress' often stated goal of expanding broadband service to every household in the country.[15]

## IV. CONCLUSION

NTCA shares the Commission's goal of helping to secure the nation's communications infrastructure from cyber threats. Any actions taken to fulfill this goal, however, need to be within the Commission's authority and avoid duplicating actions already taken by other federal agencies. The Commission should also consider the impact any equipment certifications would have on existing equipment delays and avoid any retroactive application without funding to compensate providers for the cost of removing and replacing identified equipment.

Respectfully submitted,


By: */s/ Michael Romano*
Michael Romano
Jill Canfield
Tamber Ray

4121 Wilson Boulevard
Suite 1000
Arlington, VA 22203

703-351-2000 (Tel)

[15] *See, e.g.*, *Inquiry Concerning Deployment of Advanced Telecommunications Capability to All Americans in a Reasonable and Timely Fashion*, GN Docket No. 20-269, Fourteenth Annual Broadband Deployment Report (Jan. 19, 2021), ¶ 1 ("Over the last four years, the Commission's top priority has been closing the digital divide, in recognition that high-speed broadband and the digital opportunity it brings are increasingly essential to innovation, economic opportunity, healthcare, and civic engagement in today's modern society."). *See also* FCC, NTIA and USDA Announce Interagency Agreement to Coordinate Broadband Funding Deployment, *News Release* (June 25, 2021) ("Access to reliable, affordable high-speed broadband is critical to the economic well-being of communities and small businesses across America.").