Before the
Federal Communications Commission
Washington, DC 20230

In the Matter of	)	
	)	
Protecting Against National Security	)	WC Docket No. 18-89
Threats to the Communications Supply	)	
Chain Through FCC Programs	)	

COMMENTS OF
NTCA–THE RURAL BROADBAND ASSOCIATION

I. INTRODUCTION AND SUMMARY

NTCA–The Rural Broadband Association ("NTCA")[1] hereby submits these comments in response to the Second Further Notice of Proposed Rulemaking issued by the Federal Communications Commission ("Commission") in the above-referenced proceeding.[2] In the *Notice*, the Commission seeks comment on proposals to create a new list of communications equipment and services ("Covered List"), pursuant to the Secure and Trusted Communications Networks Act ("Secure Networks Act"), that communications providers would be prohibited from using any federal subsidies to purchase or maintain.

[1] NTCA represents approximately 850 independent, community-based telecommunications companies and cooperatives and more than 400 other firms that support or are themselves engaged in the provision of communications services in the most rural portions of America. All NTCA service provider members are full service rural local exchange carriers ("RLECs") and broadband providers, and many provide fixed and mobile wireless, video and other competitive services in rural America as well.

[2] *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Declaratory Ruling and Second Further Notice of Proposed Rulemaking, WC Docket No. 18-89 (July 16, 2020) ("*Declaratory Ruling*" or "*Notice*").

NTCA supports the creation of a list of prohibited equipment and services to offer much needed clarity to communications providers as they build out and maintain their networks. To ensure providers have the most complete information available, however, NTCA encourages the Commission to include in the Covered List not only communications equipment and services identified by the Commission as posing a threat to national security but also any equipment and services separately identified as a threat to national security by other federal agencies or departments. NTCA further encourages the Commission to work with NTIA and other federal agencies and departments to establish a two-way information sharing program between providers and government officials.[3]

II. ALL COVERED EQUIPMENT AND SERVICES SHOULD BE INCLUDED IN A LIST PUBLISHED BY THE COMMISSION.

The Commission seeks comment in the *Notice* on the process and procedures to use when incorporating determinations by other government agencies onto the Covered List, including equipment or services identified in section 889(f)(3) of the 2019 NDAA.[4] As an initial matter, NTCA recommends the Commission use the same procedures for including communications equipment and services on the Covered List, whether the names of such equipment and services come from other agencies, that it used to designate Huawei and ZTE as covered entities. Specifically, the Commission should release an Order identifying all communications equipment or services placed on the Covered List, as identified by the Commission and/or other federal

[3] *See, e.g.*, *Promoting the Sharing of Supply Chain Security Risk Information Between Government and Communications Providers and Suppliers*, NTIA Docket No. 200609-0154, 85 Fed. Reg. 35919 (June 12, 2020); *Notice, Extension of Comment Period*, NTIA Docket No. 200609-0154, 85 Fed. Reg. 40625 (July 7, 2020) ("NTIA Request for Comment").

[4] *Notice* at ¶¶ 33-35.

agencies or departments. This will allow advanced communications providers to look to the Commission's list as the single source for covered entities, equipment and service. Such notice by the Commission is essential as many advanced communications providers – especially smaller operators – do not have the resources to track multiple government agencies and departments for determinations of covered equipment and services due to the many different agencies or departments with authority to make such a determination and the unpredictability of when such determinations will be made public. This is all the more important given that advanced communications providers face a significant risk of being found – by the Commission – in noncompliance with the Commission's rules governing covered equipment and services, up to and including forfeiture, if they do happen to miss *another agency's or department's* determination that certain equipment or services have been deemed a threat to national security.[5]

NTCA also recommends the Commission follow the same process for designating equipment or services to be placed on the Covered List as the Commission used for designating Huawei and ZTE as covered entities. Specifically, the Commission should issue an Order containing an initial designation that equipment and/or services identified in the Order pose a threat to national security and allow for a public comment period on such initial designation.[6] This would provide not only for consistency in the designation of companies, equipment and services as "covered," but also provide advanced communications providers with awareness that

[5] *See* Notice at ¶¶ 57-58 ("[T]he Commission would have authority to subject those found in violation of the Secure Networks Act to forfeiture…. Separately, section 7(b) [of the Secure Networks Act] requires the repayment of funds disbursed per the [Secure Networks Act] reimbursement program … if they are found to have violated … the Commission's regulations.")

[6] *See, e.g.*, *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Report and Order, Further Notice of Proposed Rulemaking, and Order, WC Docket No. 18-89 (Nov. 26, 2019), ¶ 43.

such equipment, services and/or entities are on the cusp of being deemed a threat to national security and thereby allow the providers as much time as possible to begin seeking replacement solutions or, if they have not yet purchased the identified equipment or services, to look to other equipment and services for their needs.

III. ADVANCED COMMUNICATIONS PROVIDERS NEED ADEQUATE NOTICE PRIOR TO BEING EXPECTED TO REPLACE EXISTING EQUIPMENT OR SERVICES.

The Commission proposes in the *Notice* to prohibit advanced communications providers from using USF funds "to purchase, rent, lease, otherwise obtain, or maintain any covered equipment and services identified and published on the Covered List" beginning 60 days following the date on which such equipment or services are placed on the Covered List.[7] Given the nature of procurement and capital investments, 60 days is wholly insufficient to allow providers to identify suitable replacement equipment and services, much less to obtain replacement equipment and then remove and replace all affected equipment in their network. As for how much time providers should receive to replace covered equipment and services, NTCA suggests that instead of a firm deadline, advanced communications providers should continue receiving USF support until either federal funding is available to reimburse affected providers for the cost of replacement equipment and services or the provider replaces the equipment or service in the normal course of business.[8]

Few, if any, providers receiving USF support (referred to as eligible telecommunications carriers or "ETCs") have the funds available to remove and replace existing equipment outside of

[7] *Notice* at ¶ 48.

[8] This should apply *both* with respect to the removal and replacement of prohibited equipment *and* to the ability to repair such equipment while still being used in the network pending replacement.

the normal upgrade cycle. If the Commission requires ETCs to remove and replace covered equipment prior to the normal upgrade cycle, without reimbursement for the cost of doing so, customers who depend upon the networks built by leveraging USF funds will suffer the most due to the crushing burden the cost of replacement would impose on these providers' operations, which already operate on razor thin margins, as well as the service disruptions that will almost certainly follow.

A 60 day replacement deadline is also inconsistent with the Commission's proposal to require advanced communications providers to report to the Commission within 60 days of release of an updated Covered List if they have covered equipment and/or services in their network.[9] There is little reason to require providers to report the existence of covered equipment and services in their network if they must also rip out that very same equipment at the same time.

The Commission can reduce the costs to providers, government and consumers of having to replace covered equipment or services by continuing to work with other federal agencies to establish a two-way information sharing program between government and providers.[10] The earlier the government makes providers aware of concerns with a supplier or vendor, the sooner providers can begin looking into alternative products and services rather than waiting to replace the same equipment and services after they appear on the Covered List. Information sharing can also help avoid or minimize security concerns that lead to the equipment and services being placed on the Covered List in the first place. For example, advanced communications providers – and their customers – would benefit from the federal government sharing information with

[9] *Notice* at ¶¶ 52-55.

[10] *See, e.g.*, n. 3 *infra*.

them regarding vendors suspected of, or with a history of, behavior detrimental to national security.

Receiving information regarding potential security concerns early would allow providers to consider such information when purchasing or leasing equipment or services, thereby potentially avoiding the need to replace such equipment or services after they have already been put in place and, possibly, after some damage to national security has already taken place. The Department of Homeland Security ICT Supply Chain Task Force Information Security Working Group, for example, found that in addition to providers' receipt of security risk information from the federal government, having the ability to share equipment or product security concerns with other providers or the federal government early, and prior to the federal government publicly identifying a security threat, can minimize disruptions to providers' operations.[11]

IV. CONCLUSION

NTCA continues to support strategic steps to manage cybersecurity risks in our nation's communications networks. To further this goal without interrupting critical broadband and voice services, however, NTCA encourages the Commission to include in the Covered List all equipment and services deemed a threat to national security, regardless of the agency or department that identified such equipment or services as being a threat. This will reduce not only the compliance risk of providers of missing an agency's determination but also the substantive risk that problematic covered equipment and services could remain in some providers' networks due to the provider missing one agency's or department's determination. Additionally, providers need more than 60 days to identify, obtain and install replacement

[11] *See* Comments of Communications Sector Coordinating Council, NTIA Request for Comment, July 28, 2020.

equipment and should instead be permitted to continue receiving USF funds until either government funding is available to reimburse providers for the cost of replacing covered equipment or services or the provider replaces such equipment or services in its normal course of upgrades. Finally, NTCA encourages the Commission to continue to actively pursue two-way information sharing efforts with other agencies and providers. All of these actions combined are necessary to achieve the Commission's and providers' common goal of protecting national security.

Respectfully submitted,

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

4121 Wilson Boulevard, Suite 1000
Arlington, VA 22203

703-351-2000 (Tel)