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

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

REPLY COMMENTS OF THE RURAL WIRELESS ASSOCIATION, INC.

The Rural Wireless Association, Inc. ("RWA") submits these reply comments in response to the comments and other submissions filed in the above captioned proceeding in response to the *Declaratory Ruling and Second Further Notice of Proposed Rulemaking*[1] adopted by the Federal Communications Commission ("FCC" or "Commission") on July 16, 2020 seeking comment on how it should incorporate Sections 2, 3, 5, and 7 of the Secure Networks Act[2] into its supply chain rulemaking.

The vast majority of comments submitted in response to the Second FNPRM make it abundantly clear that the Commission needs to adopt a transparent process. Transparency is welcomed by RWA in the Commission's maintenance of a Covered list, its prohibition on federal subsidies, its required reporting obligations, and its enforcement process. RWA and its rural carrier members seek further clarity from the Commission on the following topics below.

I. FCC SHOULD ADOPT BROAD DEFINITIONS TO PROMOTE FLEXIBILITY

[1] *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, Declaratory Ruling and Second Further Notice of Proposed Rulemaking*, WC Docket 18-89, FCC 20-99 (*Second FNPRM*).

[2] Pub. L. 116-124, 133 Stat. 158 (2020) ("Secure Networks Act").

To effectively monitor potentially threatening communications equipment and services, the Commission needs sufficient flexibility to be able to identify certain communications equipment and services. To that end, RWA joins Dell[3] in supporting the FCC's proposed definition of "communications equipment or service" as "any equipment or service that includes or uses electronic components that is essential to the provision of fixed or mobile advanced communications service with connection speeds of at least 200 kbps in either direction."[4] This definition provides the FCC with the flexibility it needs as technology evolves so that regulations do not lag behind technological developments. It also puts suppliers and vendors on notice as to which of their equipment and services are subject to scrutiny which, in turn, means that carriers will be able to work with their vendors and suppliers to more effectively shift contractual liability and indemnification in a manner that ensures that carriers are reimbursed for any future unsecure equipment and services by the terms of contracts rather than the American taxpayer. RWA notes that one commenter argued that the definition was too narrow[5] and another argued it was too broad.[6] Both of these concerns are curbed by the FCC's authority to either identify certain equipment and services as prohibited or designate an entity as prohibited. By adopting a rule that is broad enough to encompass individual components or an entire entity, the FCC has

[3] Dell Technologies, Inc. ("Dell") at p. 1 ("[Dell] supports the Commission's proposal for providing a bright-line rule for 'communications equipment and services,' to include all services and equipment used in fixed and mobile broadband networks, provided they use or include electronic components. This definition would make it universally clear for compliance purposes.").

[4] *Second FNPRM* at Appendix A, § 1.40001(c).

[5] Competitive Carriers Association ("CCA") Comments at p. 3-4 ("…the Commission cannot alter the statutory language and need not adopt a cramped interpretation in order to implement the Program, particularly given the Secure Networks Act's expansive aim…the Commission should adopt rules that interpret the statutory language as it most accurately reflects the broad participant pool Congress intended for the program.").

[6] CTIA Comments at p. 9 ("This proposed definition is unduly broad and lacks sufficient nexus to an ascertainable risk to U.S. telecommunications networks.").

flexibility to react to preserve the security of U.S. communications networks and secure the supply chain.

II. THE RECORD OVERWHELMINGLY SUPPORTS A REQUIREMENT THAT THE COMMISSION PROVIDE PUBLIC NOTICE OF ANY UPDATES MADE TO THE FCC'S COVERED LIST

In the *Second FNPRM*, the Commission proposed that when an appropriate body[7] determines that certain equipment or services pose a national security threat the announced determination by that agency is adequate notice to the public and no separate notice is needed from the Commission that the equipment or service will be added to the Covered list.[8] A majority of commenters expressly rejected this notion and argued that the FCC should provide separate notice to the public.[9] In agreement with those commenters, RWA proposes that when the FCC incorporates external determinations into its Covered list, or make other changes to its list, the Commission should provide a separate notice to the public that such changes are being made to the Covered list. Many rural carriers do not have sufficient resources to monitor the

[7] *Second FNPRM*, para. 31 (defining an appropriate body as any executive branch interagency body with appropriate national security expertise, the Department of Commerce (DOC), or any appropriate national security agency).

[8] *Id*., para. 38 ("We expect that any determinations covered under sections 2(c) [(Covered list)] will be publicly released by the original decisionmaker. If such a determination is public, we do not believe the Commission must issue any notice regarding our receipt of this determination. We seek comment on this understanding.").

[9] CITA Comments at p. 16 ("Nor should the Commission automatically add to the Covered List upon a finding by another agency. It should provide notice of additions or changes to the Covered List."); Huawei Technologies Co. ("Huawei") Comments at p. 18 ("…[t]he Commission must provide notice of both the specific determinations by other agencies upon which it intends to rely, and its intent to include equipment or services on the Covered List, before acting to add equipment or services…"); NCTA – The Internet & Television Association ("NCTA") Comments at p. 9 ("First, the Commission should provide as much up-front clarity and notice as is possible with respect to the identity of the Federal agencies and inter-agency bodies that can render national security risk determinations under the Secure Networks Act."); NTCA – The Rural Broadband Association ("NTCA") Comments at p. 2-3 ("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 agencies or departments… Such notice by the Commission is essential as many advanced communications providers…do not have the resources to track multiple government agencies and departments for determinations of covered equipment and services…").

determinations made by multiple governmental bodies and agencies and thus a notice from the Commission itself will serve the public interest.

III. PROVIDERS SHOULD HAVE SUFFICIENT TIME TO TRANSITION AWAY FROM EQUIPMENT AND SERVICES ADDED TO THE COVERED LIST IN THE FUTURE

Under the proposed rules, providers will be barred from using their federal subsidies to purchase and maintain communications equipment and service that are placed on the Covered list 60 days after it is published.[10] The proposed 60-day grace period is insufficient as many rural carriers do not have the resources to make such potentially drastic modifications to their networks in such a short period of time, especially if they are not given prior notice, as currently proposed by the Commission. Both CCA's "milestone" approach[11] and NCTA's "safe harbor" approach[12] are measures that the Commission could implement that would effectively alleviate these concerns. RWA suggests that the Commission adopt one of the proposals or some similar alternative.

IV. FCC SHOULD IMPLEMENT RULES TO PROMOTE SECURING AND FUTURE-PROOFING OF NETWORKS

[10] *Second FNPRM* at Appendix A § 54.10(c) ("The prohibition in paragraph (a) of this section applies with respect to any covered communications equipment or service beginning on the date that is 60 days after the date on which such equipment or service is placed on a published list pursuant to section [x] of this chapter.")

[11] CCA Comments at p. 6 ("CCA urges the Commission to implement this aspect of the Program in a way that allows carriers to *demonstrate they are making progress and meeting milestones* to receive the necessary time to transition away from funding or new equipment installation while preserving connectivity for their customers.") (emphasis added).

[12] NCTA Comments at p. 13 ("Alternatively, the Commission should consider creating a *safe harbor from the effect of the subsidy prohibition for providers that are making a reasonable, good-faith effort to transition away from newly-banned equipment* but cannot meet the 60-day removal timetable without significant disruptions to network operations or service delivery.") (emphasis added).

The Commission should adopt rules with the goal of encouraging the future-proofing of networks. With many rural providers overhauling their entire networks, it is imperative that these providers install equipment and services that are easily adaptable to future generation technologies at a relatively low-cost and that network monitoring for security threats be adopted as best practices. To help achieve this objective, RWA agrees with some of the recommendations made by Dell for securing and monitoring the security of networks. For example, security and threat protections should be integrated into new deployments and equipment should provide manageable solutions to entities of all sizes.[13]

RWA looks forward to continued discussions with the FCC on developing procedures and rules to efficiently and quickly replace and remove unsecure equipment and services in U.S. communications networks and for implementing security measures that will protect U.S. networks that interconnect with each other both domestically and that connect to other networks abroad.

Respectfully submitted,

RURAL WIRELESS ASSOCIATION, INC.

By: */s/ Carri Bennet*

Carri Bennet, General Counsel
Stephen Sharbaugh, Legislative and Policy Analyst
5185 MacArthur Blvd., NW, Suite 729
Washington, DC 20016
(202) 551-0010
legal@ruralwireless.org

September 14, 2020

[13] Dell Comments at p. 2 ("Dell Technologies recommends that equipment is automatically assured to provide solutions that are easy to manage for organizations of all sizes… Threat protections must also be seamlessly integrated and not rely upon current deployment patterns that rely on each organization to have skilled expertise. As such, Dell Technologies believes that providing trusted infrastructure to readily detect and prevent threats is critical towards supplying the vast 5G ecosystem.").