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

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

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 Federal Communications Commission's ("FCC" or "Commission") *Public Notice*[1] seeking comment on Section 4 of the Secure and Trusted Communications Act of 2019.[2]

The vast majority of comments submitted in response to the *Public Notice* make it abundantly clear that the FCC needs to manage any potential covered company equipment replacement and removal program in a swift and comprehensive manner. Beyond that, there are differences in opinion on what the Secure Networks Act requires of the FCC in implementing its replacement-and-removal process. With respect to the mandated "suggested replacement list,"[3] RWA and other commenters agree that the Commission should create a list of acceptable categories of equipment and services supplied by approved vendors. As discussed below, the burden of supplying accurate information for the list should fall on the vendors and manufacturers, not the carriers. Furthermore, the funds from the reimbursement program

[1] *Applicability of Section 4 of the Secure Networks Act to the Rulemaking on Protecting Against National Security Threats to the Communications Supply Chain*, DA 20-406, WC Docket No. 18-89 (rel. Apr. 13, 2020) ("*Public Notice*").
[2] Pub. L. 116-124, 133 Stat. 158 (2020) ("Secure Networks Act").
[3] Secure Networks Act, Section 4(d)(1).

should be distributed equitably and that disbursement should go to all providers of "advanced communications service" with covered company equipment, and not just those ETCs receiving USF support, as established by the Secure Networks Act.[4] Commenters also discussed whether reimbursement should be permitted for equipment upgrades that include components compatible with 5G services. Such upgrades should be fully reimbursed if a replacement of "like-wise" equipment is otherwise practically infeasible.

RWA and its rural carrier members stand ready to support a nationwide replace and remove mandate, but in order for it to be effective, the aforementioned elements need to be adopted. Furthermore, until the reimbursement program is appropriated funding from Congress, the Commission needs to refrain from formally designating Huawei and ZTE as "covered companies" and continue to provide USF support to ETCs throughout the duration of the rulemaking and transition periods so that rural wireless carriers can keep their rural customers and those roaming on their networks connected.

I. The "Safe List" Should Both Identify Vendors and the Categories of Equipment and Services Offered by Such Vendors

The Secure Networks Act mandates that the Commission create either a list of suggested replacements of equipment and services or a list of categories of replacement equipment and services.[5] Such a "safe list" is mandatory, contrary to some commenters' proposals.[6] A "deny list" is contemplated

[4] *Id.*, Section 9(1).

[5] Secure Networks Act, Section 4(d)(1)(A) states: "The Commission shall develop a list of suggested replacements of both physical and virtual communications equipment, application and management software, and services or categories of replacements of both physical and virtual communications equipment, application and management software and services."

[6] Computing Technology Industry Association ("CompTIA") Comments at p. 6 ("Ideally, decisions regarding particular suppliers of concern would follow risk-based approaches that might prohibit specific suppliers based on evidence of wrongdoing – a 'deny list' rather than an 'approve list'…"); NTCA – The Rural Broadband Association ("NTCA") Comments at p. 4 ("NTCA encourages the Commission…to provide a list of companies identified by the 2019 NDAA, rather than attempting to create a list of permissible hardware and software components, their manufacturers, and any names under which such products and services might be sold."); USTelecom Comments at p. 6 ("…there is no need to create a separate list of 'allowable' equipment in the

elsewhere in the Secure Networks Act, specifically Section 2(a), which requires the publication of a list of covered companies communications equipment or services that are forbidden.[7] This list is separate. Merely stating that a vendor is automatically on the "safe list" if it is not on the "deny" list is not legal under the Secure Networks Act. It is within the Commission's discretion only to decide whether the suggested replacements or "safe list" specifies particular equipment and services supplied by vendors or specifies categories of equipment and services supplied by vendors. Thus, it is not permitted by the statute to simply provide a list of "approved" vendors, as recommended by the Competitive Carriers Association ("CCA").[8] A list only composed of "approved" vendors would either result in: (1) an overly inclusive process that approves every vendor, that is not Huawei or ZTE, increasing the potential of this situation arising again in the future; or (2) leaving vendors out of the process, who are not approved initially, because they are new entrants or were unaware that there was an approval process requiring their participation.

An approach is needed to quickly and securely replace covered company equipment that currently continues to pose a security threat to American communications networks. The law would best be implemented by the Commission developing a list identifying approved vendors and the categories of equipment and services provided by such vendors. This approach is partially supported by CTIA,[9]

supply chain—any equipment that is not derived from a manufacturer designated as a national security threat should be 'allowed.'").

[7] Secure Networks Act, Section 2(a) states: "Not later than 1 year after the date of the enactment of this Act, the Commission shall publish on its website a list of covered communications equipment or services."

[8] CCA Comments at p. 9 ("CCA recommends that the Commission approve trusted vendors, rather than approve specific pieces of equipment.").

[9] CTIA Comments at p. 8 ("…the Commission should consider creating categories of suggested replacements, rather than listing "the precise names of the equipment and services from those companies that are eligible for reimbursement.").

Ericsson,[10] Juniper Networks ("Juniper"),[11] and the Open RAN Policy Coalition ("Coalition")[12] who seek to use a list of categories of equipment and services, but not name the vendor. RWA believes that identifying the vendor is also critical and it would not be a heavy lift to do so. Under RWA's approach there would be simplicity for vendors and needed specificity for carriers.[13] The Commission could serve as a clearinghouse to collect this information and provide it through a FCC-run portal, allowing vendors to simply indicate (by checking a box) the categories of equipment and services they offer since they are in the best position to do so. The information could be compiled into a list that is publicly released, accessible to carriers and updated periodically as new vendors and vendors' new categories of equipment and services become available. The FCC should create a simple process to allow the vendors to indicate the categories of equipment and services they offer. RWA has attached a chart, "Proposed Categories of Equipment/Services List", under Attachment A, breaking down the suggested categories of equipment and services that each vendor could check off in the portal so that the FCC could review and then approve by publishing on its website.

While moving expeditiously to fund the replacement of covered company equipment and services, the Commission should also adopt safeguards to avoid future security threats to American communications networks. Such safeguards should require vendors to certify that their equipment and services are secure and do not pose national security risks. Specifically, vendors could certify under penalty of perjury that their equipment complies with the law with respect to network security. In furthering that objective, the

[10] Ericsson Comments at p. 10 ("The Secure Networks Act provides the Commission the option of developing a list of 'categories of replacements,' and the Commission should take this approach rather than naming specific 'suggested' suppliers…").
[11] Juniper Comments at p. 2 ("With respect to the substance of the replacement list, we recommend that the Commission first develop a list of product categories (e.g., routers, switches, firewalls) and then include within each category a list of secure, open, and industry-led standards, best practices, and protocols.").
[12] Coalition Comments at p. 9 ("…the Commission should develop a list of categories of suitable replacement equipment and services, rather than a list of specific named suppliers or particular equipment and services.").
[13] RWA members consist of rural carriers and vendors serving these carriers. Together the carriers and vendors have developed this approach through thoughtful consideration of each other's costs, capabilities and resources. Together, RWA's carriers and vendors have arrived at a workable solution that meets the letter of the law without also overburdening the FCC.

Commission should require vendors to certify that they have not provided "white-labeled" equipment or services from any vendors deemed to be covered companies. A vendor could make this certification when indicating, in the portal, which categories of equipment and services it provides. It is infeasible, if not impossible, for rural carriers to determine whether a vendor's equipment, in whole or in part, is actually manufactured by either Huawei or ZTE (or a potential covered company named in the future). While the carriers have a responsibility to act diligently, the duty should be on the vendors to be transparent about their equipment and services as they are the only entities that have access to information about the actual source of the equipment and services. This certification must be required of vendors when submitting its list of categories of equipment and services, under penalty of the laws of the United States. The act of certifying will provide carriers the necessary tool to hold a vendor legally accountable to the carrier should a vendor later be deemed to have either "miscertified" or later become a "covered company."

The Commission should also adopt a "safe harbor" for carriers, in the event they are sold equipment or services that are later determined to pose a national security threat. If a carrier purchases equipment or services, from a listed vendor, that fall within the categories of that vendors' approved equipment and services, it should be presumed that the carrier acted responsibly in choosing to purchase that vendor's equipment or services. Rural carriers lack the resources to extensively vet vendors' supply chain and thus must rely on the Commission's list in replacing their covered company equipment and services.

II. Reimbursement Funds Should Be Distributed Equitably

In disbursing reimbursement funds, as mandated by the Secure Network Act,[14] the Commission should distribute funds "proportional to need" among participants if there is an insufficient amount of funds initially appropriated. "Participants" in the reimbursement program should include all "provider[s] of

[14] Secure Networks Act, Section 4(a).

advanced communications equipment."[15] CCA,[16] NetNumber, Inc. ("NetNumber"),[17] Northern Michigan University ("NMU"),[18] NTCA,[19] and PTA-FLA, Inc. ("PTA-FLA")[20] all are in agreement with RWA that eligible entities for the reimbursement program should include all providers of advanced communications services. The Secure Networks Act only limits eligibility in three ways. Eligible entities must: (1) have two million or fewer customers;[21] (2) be a provider of "advanced communications service;"[22] and (3) make the required certifications outlined in Section 4(d)(4).[23] In addition, even though non-ETC providers might be exempt from the Commission's mandated removal of existing Huawei and ZTE equipment, NMU accurately points out that such providers will be significantly harmed by the declining Huawei US market as they will be unable to purchase the necessary hardware and software to maintain their current networks.[24] The replacement of covered company equipment for non-ETCs is practically essential and many non-ETCs

[15] *Id*., Section 4(b).

[16] CCA Comments at p. 2-3 ("The Commission need not alter or restrict that language [in the Communications Act and referenced in the Secure Networks Act] in order to implement the Program, particularly given that the Secure Networks Act's expansive aim to 'provid[e] for the establishment of a reimbursement program for the replacement of communications equipment or services posing' national security risks.") (arguing that the definition of advanced communications providers is plain on its face).

[17] NetNumber at p. 7 ("While this definition potentially covers many network solutions, the Commission should interpret ACS [i.e. advanced communications service] in a way that covers all equipment and services that could pose a national security risk now or in the future.").

[18] NMU Comments at p. 2 ("As the FCC develops a reimbursement program to offset transition costs to new equipment, NMU [as a non-ETC] believes it should be eligible for such funds.") (arguing that non-ETCs, that meet the statutory definition of providing advanced communications services, should be included).

[19] NTCA Comments at p. 2-3 ("…the statute applies to more than ETCs alone – the Act expressly makes eligible for 'rip and replace' funding any 'provider of advanced communications services,' without reference to ETC status, that has 2 million or fewer customers and that makes certain certifications.").

[20] PTA-FLA Comments at p. 1 ("The Secure Networks Act establishes a program that is not only not targeted exclusively at ETCs…").

[21] Secure Networks Act, Section 4(b)(1).

[22] Secure Networks Act, Section 4(b).

[23] Secure Networks Act, Section 4(b)(2) (The required certifications are: (1) the applicant has developed a plan and timeline for the permanent removal, replacement, and disposal of its covered company equipment or services; (2) the applicant will not "purchase, rent, lease, or otherwise obtain covered communications equipment or services, using reimbursement funds…;" and (3) the applicant will consult and consider standards and guidelines set forth by the National Institute of Standards and Technology.).

[24] NMU Comments at p. 2.

could have difficulty covering those costs and thus should be included in the reimbursement program. This proceeding began for the purpose of protecting American communications networks and that can only be achieved by eliminating covered company equipment and services entirely.

As proposed by NetNumber, funds could be disbursed equitably by using reimbursement "caps" to ensure that carriers are fairly compensated for their costs incurred in replacement-and-removal.[25] These reimbursement caps could be determined by considering both the size of the network deployment and the service provider type.[26] As NetNumber explains in its comments, some carriers may have spent more on covered company equipment than other carriers and because of the type of services a provider offers, one provider may spend more on replacement costs because the equipment it purchases includes 5G or is 5G ready.[27] In imposing these "caps," the FCC should recognize the need for eligible carriers to have maximum flexibility to deploy replacement equipment or offer replacement services in the most commercially efficient ways and at the most critical locations. In addition, for those carriers who do not get enough funding to cover their replacement costs and decide to exit the market, funding should still be made available to reimburse them for the removal and destruction of the covered equipment so it does not end up in the supply chain again and sold as used equipment or replacement parts. Once a sufficient amount of funds is appropriated, carriers should be *fully* reimbursed for all of their replacement, removal, and disposal costs.

The Commission should also consider adopting a cost catalog of preapproved reimbursement expenses to aid carriers in planning their replacement-and-removal process. A cost catalog would expedite the application review process, allowing rural carriers to begin their replacement of covered company equipment shortly after funding is appropriated by Congress. Given that COVID-19 has delayed the

[25] NetNumber Comments at p. 9 ("…the Reimbursement Program should include funding caps to advance the objective of replacing covered equipment and services nationwide without favoring any particular region or customer segment.").
[26] *Id*.
[27] *Id*.

appropriation for the Secure Networks Act, and presumably will continue to delay it, the Commission should have a sufficient amount of time to create a cost catalog and seek comment accordingly.

III. Reimbursement Should Apply to Upgrades to 5G Services

It is imperative that participants are *fully* reimbursed for the costs of replacing their equipment and services, even if such replacement is accomplished via upgrades that include components that support 5G services. Contrary to the views expressed by USTelecom,[28] rural carriers should not be penalized for using Huawei or ZTE equipment and services in their networks. Rural carriers followed, in good faith, the rules set by the Commission in the Mobility Fund Phase I ("MF I") auction and, in doing so, expended their limited funds, derived from a reverse auction, to provide high-cost service to areas that today would likely still be unserved. In order to make these high-cost projects economically feasible, these rural carriers typically followed a competitive bidding process and accepted the lowest bid submitted by qualified vendors. This resulted in the purchases of Huawei and ZTE's low-cost equipment. At the time, neither Huawei nor ZTE had been publicly deemed a national security risk. Now, through no fault of their own, rural carriers' Huawei and ZTE equipment have been determined to pose an unacceptable risk to U.S. national security. USTelecom asserts, without any basis, that rural carriers are gaining a "competitive advantage."[29] But rural carriers are in no position to financially "take advantage" of this process. These carriers are simply trying to serve their customers and if rural carriers "had invested wisely," presumably by purchasing more expensive equipment, as suggested by USTelecom, many more Americans would be without broadband service because the limited funds would not have gone as far. That approach would have been "unwise" and therefore totally counter to the MF I policy objectives. The MF I reverse auction was capped at $300 million

[28] USTelecom Comments at p. 8 ("Some market participants already made the decision to spend more—sometimes substantially more—to avoid using equipment from Huawei and ZTE in the first place and carriers who need to replace parts of their networks should not have a competitive advantage over those who invested wisely in the first place.").

[29] *Id*.

and rural carriers were trying to go from 2G to 3G or 3G to 4G LTE. MF I also had a strict performance requirement to provide coverage to no less than 75% of every road and "pig trail" in the eligible census area. Perhaps USTelecom and its larger members have forgotten the difficulties and rigors involved in providing services to low density markets since, by and large, they long ago abandoned those areas in favor of investments in serving major metropolitan areas across the country and around the globe which, in turn, has contributed heavily to the vast digital divide that exists today. The limited funds and the reverse auction required resourcefulness and, at the time the auction was conducted, the U.S. and China (who heavily subsidized Huawei and ZTE) had a strong relationship. As such, RWA takes umbrage with USTelecom's revisionist history. The FCC has long encouraged investment in high-cost, rural areas and should continue to encourage such investments in the future, especially as the Commission attempts to close the digital divide and bring 5G to all Americans. Accordingly, to the extent 5G components are included in the replacement of 3G or 4G LTE equipment and services, the cost of such components should be reimbursed.

RWA firmly believes that carriers should be reimbursed fully for upgrades to 5G services. This notion is also supported by PTA-FLA.[30] Replacing "like-wise" equipment is not always feasible and by not allowing reimbursements for upgrades to 5G services, when replacing like-wise equipment is otherwise infeasible, the FCC will put rural areas years behind in the race to 5G. Reimbursing these costs is also a more efficient use of taxpayer dollars. It would be a waste of hard-earned taxpayer dollars to force rural carriers to deploy end-of-life or near end-of-life equipment and then later use more taxpayer dollars, in the form of Universal Service Funds, such as contemplated in the Rural Digital Opportunity Fund ("RDOF") and 5G Fund for Rural America programs, to replace that equipment with 5G equipment. Reimbursement

[30] PTA-FLA Comments at p.4 ("The upshot is that the statutory scheme envisions reimbursement for removal, replacement and disposal of new equipment but recognizes that older generation equipment may be removed and replaced with newer generation equipment.").

funding should be forward-looking and made available in a way that allows rural carriers to prepare their networks for the advent of 5G, including network virtualization and other such advancements. This is the only practical way to ensure that deployed networks in currently served rural markets can eliminate the current security vulnerabilities, while keeping those same rural networks from falling behind in the efforts to extend the benefits of rapidly evolving technologies to rural markets. Under this approach, rural carriers will be able to make meaningful contributions to the collective efforts aimed at "Keeping Critical Connections" – a key public interest goal touted by the Commission.

RWA looks forward to continuing to work with the Commission on this vital proceeding to secure America's communications supply chain while keeping rural America connected.

Respectfully submitted,

RURAL WIRELESS ASSOCIATION, INC.

By: */s/ Carri Bennet*

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

June 4, 2020

Attachment A

Proposed Categories for Equipment/Services List[31]

Category	Description
Access	Equipment associated with providing and controlling end-user access to the network over the "last mile," "local loop," or "to the home." (ex. OLTs, DSLAMs, MSANs, ONUs, Cabinets, CPE, Terminating/access WDM/OTN)
Distribution	Middle-mile, backhaul, or radio area network (RAN) equipment layered between the access and core layers of the network in which network traffic management policies are defined and enforced. (ex. RAN (RRU, BBU, etc.), antennas, shelters, microwave, routers, switches, Metro WDM/OTN)
Core	Backbone infrastructure that provides for fast routing of traffic with minimal processing and interconnection to other networks. (ex. EPC, IMS, Datacenter Gear, Backbone WDM/OTN)
Software	For conceiving, specifying, designing, programming, testing, maintenance and developing equipment applications, components or systems that are continuously used. (ex. OSS/BSS, EMSs)
Services	One time design, implementation, installation, testing and other costs to deploy gear, ongoing operational services

[31] "Network Categorization." Federal Communications Commission, Information Collection. Modified Feb. 14, 2020. Accessed at https://us-fcc.app.box.com/v/NetworkCategories.