Before the
DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration
Washington, D.C. 20230

Notice and Request for Comment	)	
	)	
Promoting the Sharing of Supply Chain Security Risk Information Between Government and Communications Providers and Suppliers	)	Docket No. 200609-0154

COMMENTS OF COMPETITIVE CARRIERS ASSOCIATION

Competitive Carriers Association ("CCA")[1] respectfully submits the following comments in response to the National Telecommunication and Information Administration's ("NTIA") Request for Public Comment[2] to inform the implementation of a supply chain information sharing program pursuant to Section 8 of the Secure and Trusted Communications Network Act of 2019 ("Secure Networks Act").[3] CCA and its members strongly support a robust information-sharing system and we appreciate the opportunity to offer input on its implementation.

[1] CCA is the nation's leading association for competitive wireless providers and stakeholders across the United States. Members range from small, rural carriers serving fewer than 5,000 customers, to regional and national providers serving millions of customers, as well as vendors and suppliers that provide products and services throughout the wireless supply chain.

[2] Promoting the Sharing of Supply Chain Security Risk Information Between Government and Communications Providers and Suppliers, 85 Fed. Reg. 35,919 (June 12, 2020) ("Request for Comment").

[3] Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 8, 134 Stat. 158, 168 (2020) ("Secure Networks Act").

I. INFORMATION SHARING IS VITAL TO PROMOTING NATIONAL SECURITY

CCA appreciates NTIA's efforts to establish an information sharing program as part of its implementation of the Secure Networks Act. This effort is particularly important and timely as various components of the government move to implement the statute, including moving to require replacement of covered equipment in existing networks.

As NTIA knows, many telecommunications carriers, particularly in rural America, purchased and installed equipment made by Chinese manufacturers many years ago, at a time when doing so was simply an economically rational decision without known national security implications. In some instances, the Federal Communications Commission's ("FCC") Universal Service reverse auction mechanism drove applications to the lowest cost equipment in order to obtain support, including equipment from Chinese suppliers. These carriers made decisions in good faith at the time, and are now eager for a clear path forward. CCA's members are strong supporters of protecting national security and they want to do the right thing for their communities; they just need the information necessary to do so, both today and in the future.

In recent years, as the federal government has come to identify equipment from certain suppliers as presenting national security concerns, carriers have persistently sought clear guidance from the government. CCA and its members have pressed for years for clear guidance on what equipment is prohibited, whether and how the risks may be distributed within networks and across the telecommunications ecosystem, and what the priorities are for making changes, among other questions. CCA's members have long felt that they need, and indeed deserve, clear guidance on the nature and scope of any risks, how to mitigate or eliminate the risks, and how they can plan with confidence moving forward.

As the national security risks become more prominent, CCA made extensive efforts to promote information sharing and bi-directional dialogue between industry and government. For example, last year CCA's members were able to take part in a briefing from the Senate Intelligence Committee that included leadership from multiple national security agencies. CCA also partnered with the U.S. Chamber of Commerce and the Department of Homeland Security to conduct a series of rural engagement initiatives in locations around the country. These rural engagement sessions brought together leadership from NTIA, FCC, DHS, DOJ, and other federal agencies for closed-door dialogues with industry leaders and carriers with covered equipment. In CCA's view, these sessions proved to be very positive in enabling information sharing both from government to industry and from industry to government, and CCA particularly applauds DHS's initiative in promoting this important dialogue and in helping to move the conversations outside of D.C. to locations across the country.

CCA is pleased that NTIA is leading the charge to implement an information-sharing program that will enable its members to make informed decisions about their networks. As the industry builds to widespread deployment of 5G, small and rural carriers want to expand and strengthen their networks as swiftly as possible. Clear government direction will enable them to make informed choices to ensure our networks are secure while preventing unnecessary delays that might disadvantage them competitively. Recent history confirms that it is essential that NTIA's information sharing program offer clear and regular guidance to small and rural carriers both now and in the future as national security issues arise.

II. NTIA SHOULD DEFINE THE PARAMETERS OF THE INFORMATION PROGRAM THAT BEST REFLECTS THE INTENT OF CONGRESS

The Request for Public Comment seeks comment on the term "advanced communications service" in the context of determining what entities are eligible to participate in the information-

sharing program.[4] The Secure Networks Act provides that "advanced communication service" carries the "meaning given the term 'advanced telecommunications capability'" in 47 U.S.C. § 1302:[5] "high-speed, switched, broadband telecommunications capability that enables users to originate and receive high-quality voice, data, graphics, and video telecommunications using any technology," "without regard to any transmission media or technology."[6] NTIA should adopt this language as it most accurately reflects the broad participant pool Congress intended for the program.[7]

III. INFORMATION POLICIES AND PROCEDURES SHOULD FACILITATE TWO-WAY INFROMATION SHARING AND ESTABLISH CLEAR CHANNELS OF COMMUNICATION

The following recommendations pertaining to the policies and procedures of NTIA's information sharing program reflect our members' eagerness for security risk information while accounting for potential barriers to a successful program.

a. Communications should include regular meetings and updates

To maximize the effectiveness of an information-sharing program, NTIA should employ a combination of different channels of communication that promote the two-way flow of information. It is critically important for small and rural providers to receive security threat information and guidance from the government, but it is equally important that the government

[4] Request for Comment at 35,921.

[5] Secure Networks Act § 9(10).

[6] 47 U.S.C. § 1302(d)(1).

[7] Importantly, the Secure Networks Act does not refer to the definition of "advanced communications services" in Section 3 of the Communications Act, which is different from the definition of "advanced telecommunications capability" in Section 706 of the Telecommunications Act of 1996. *See id.* § 153(1) (defining advanced communications services as "(A) interconnected VoIP service; (B) non-interconnected VoIP service; (C) electronic messaging service; and (D) interoperable video conferencing service").

be keenly informed of carriers' experiences on the ground. NTIA should consider a combination of mechanisms for information sharing, including regular meetings, as well ad hoc updates as particular issues arise.

As NTIA is aware, many of the program's carrier participants are located in rural regions throughout the country and may not possess the personnel or financial resources to attend in-person meetings in Washington, D.C. To ensure providers are kept abreast of meetings and updates from NTIA, NTIA should enlist the help of trade associations. Many small and rural carriers belong to trade associations like CCA, who often serve as the company's only point or main point of contact in Washington. NTIA could leverage the established relationships between trade associations and their members to ensure that even the smallest carriers are kept informed. Representatives from trade associations could attend meetings and assist NTIA in conveying essential information to its smallest members.

In addition to regular meetings and updates, NTIA should consider conducting field meetings throughout the country to make it easier for carriers to attend in person and build personal relationships with NTIA officials. NTIA officials also should make themselves available for direct communications with program participants. This direct contact would give participants an opportunity to resolve time-sensitive issues that arise in between regular meetings and updates and to get participant-specific support. Further, this face-to-face dialogue presents an ideal opportunity for NTIA officials to learn more about the unique challenges facing carriers throughout the country.

b. Security Risk Information Should be Readily Available to Providers

In addition to regular meetings and updates, there are several other ways NTIA should make its resources available for program participants. For example, the FCC is seeking

comment on creating a list of prohibited equipment. However, many CCA members have said that equally important would be a list of approved vendors or approved equipment. Carriers are constantly making investments in their networks and planning for additional upgrades and expansion. They want the confidence that the purchasing decisions they make today will not turn into another national security problem tomorrow. NTIA can help promote ongoing national security by helping carriers identify and acquire equipment and services that will ensure secure networks in the future.

One particularly valuable step would be an opportunity for carriers to seek information about potential vendors as part of their diligence process. For example, if a carrier is seeking to contract with a new vendor, it would be helpful for there to be a process by which the carrier could ask national security agencies whether there are any relevant national security risks that should inform their decision. And, while recognizing that there are confidentiality considerations, NTIA should consider whether there are ways to disseminate relevant information so that the entire ecosystem is aware of relevant risks. NTIA should look for ways to provide carriers with information about the specific nature of risks of equipment and suppliers and with information and whether those risks can be mitigated.

The transition to 5G creates particular opportunities to promote national security. In 5G networks, many more functions will become virtualized, and networks will leverage software on commodity hardware, or even residing in the cloud. Open RAN and virtual RAN technologies present opportunities to deploy open and interoperable interfaces that may increase the diversity of suppliers. The "intelligence" of wireless networks may also become more distributed, with certain core network functionality moving to the RAN. The increased diversity of network vendors coupled with the distributed architecture of 5G networks will place a premium on the

government being specific in identifying security risks. NTIA can help ensure that this transition is successful by communicating the specific nature of risks and helping to promote the dessimination of national security information so that 5G networks can be secure in their design and in all facets of implementation.

* * *

CCA and its members appreciate the creation of an information-sharing program that will provide the information about the security of their networks that they have sought for many years. As some of CCA's members are beginning the process of "rip and replace" to secure their networks, it is essential they have clear, informed guidance going forward to prevent future rounds of rip and replace and to ensure the security of the country's networks. As long as NTIA implements a robust information-sharing program, CCA believes that these goals will be accomplished.

Respectfully submitted,

/s Alexi Maltas

Alexi Maltas, SVP & General Counsel
Alexandra Mays, Policy Counsel
Competitive Carriers Association
601 New Jersey Ave. NW
Suite 820
Washington, DC 20001
(202)747-0711

July 28, 2020