RWA
RURAL WIRELESS ASSOCIATION

April 9, 2018

Via ECFS

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

RE: NOTICE OF EX PARTE
WC Docket No. 18-89: *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*

Dear Ms. Dortch,

The Rural Wireless Association, Inc. (RWA) has reviewed the draft Notice of Proposed Rulemaking[1] scheduled to be considered at the April 17, 2018 Open Meeting[2] with great interest. The *Draft Item* would "propose and seek comment on a rule to prohibit, going forward, the use of USF funds to purchase equipment or services from any communications equipment or service providers identified as posing a national security risk to communications networks or the communications supply chain."[3]

RWA and its members share the Commission's desire to ensure "the security of America's communications networks,"[4] and recognize the critical role that communications networks play in protecting public safety and national security. However, RWA and its members are concerned that, if adopted, the *Draft Item* would both: (1) fail to effectively protect national security; and (2) irreparably damage broadband networks (and limit future deployment) in many rural and remote areas throughout the country.

Like the Commission, RWA and its members understand that the communications network supply chain is global. That is why RWA urges the Commission to focus its efforts on the creation of a standards and testing based system, and not on imposing a costly and ultimately ineffective "country of origin" prohibitory regime that would provide nothing more than a false sense of security.

[1] *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Draft Notice of Proposed Rulemaking, WC Docket No. 18-89 (last accessed April 10, 2018) ("*Draft Item*").
[2] Press Release, *FCC Announces Tentative Agenda for April Open Meeting* (Mar. 27, 2018).
[3] *Draft Item* at ¶ 2.
[4] *Id.* at ¶ 1.

A serious defensive national cyber security strategy requires a risk management strategy and program that address the risk from all suppliers of products and services to government and critical infrastructure, including the communications sector. Additionally, any such national cyber security strategy should be applicable to all communications networks in the United States rather than targeting those relatively few communications networks funded in part by USF that use equipment from particular countries. The National Institute of Standards and Technology (NIST) Cybersecurity Framework (Framework), required for use by U.S. government agencies in a 2017 Executive Order,[5] provides a risk-analysis tool for organizations to prioritize their risk mitigation efforts in the context of their organization's business objectives and particular risk environment. NIST is expected to issue an updated version of the Framework this year that will explicitly reference the importance to an organization's risk profile of ensuring that their suppliers utilize effective supply chain risk management processes (SCRM), consistent with the principles of the Framework.

As the Commission notes in the *Draft Item*, its Communications Security, Reliability and Interoperability Council (CSRIC) has been charged with providing recommendations to ensure the security and reliability of the nation's communications systems, including telecommunications, media, and public safety networks.[6] The CSRIC IV, Working Group 4 released its Final Report on Cybersecurity Risk Management and Best Practices in March 2015.[7] This report provided guidance regarding communications providers' use of the Framework. It was presented to and adopted by the full CSRIC on March 18, 2015,[8] and the Public Safety and Homeland Security Bureau immediately sought comment on the CSRIC IV report and its cybersecurity risk management recommendations, including suggested "alternatives to better achieve the Commission's goals."[9] Several parties filed comments,[10] but to date, the Commission has taken no further action in that proceeding.

[5] Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (issued May 11, 2017) (stating "each agency head shall use The Framework for Improving Critical Infrastructure Cybersecurity…developed by the National Institute of Standards and Technology, or any successor document, to manage the agency's cybersecurity risk").

[6] *See Draft Item* at ¶ 9; *see also* FCC, Communications Security, Reliability and Interoperability Council, https://www.fcc.gov/aboutfcc/advisory-committees/communications-security-reliability-and-interoperability-council-0.

[7] CSRIC IV, *Cybersecurity Risk Management and Best Practices Working Group 4: Final Report* (March 2015) (*Working Group 4 Report*).

[8] CSRIC IV, *Cybersecurity Risk Management and Best Practices (WG 4) Final Report Presentation* (Mar. 18, 2015).

[9] Public Notice, *FCC's Public Safety and Homeland Security Bureau Requests Comment on CSRIC IV Cybersecurity Risk Management and Assurance Recommendations*, PS Docket No. 15-68, DA 15-354 (rel. Mar. 19, 2015) ("*CSRIC IV Report Public Notice*").

[10] *See* comments filed by the Telecommunications Industry Association, CTIA – The Wireless Association, WTA – Advocates for Rural Broadband, Motorola Solutions, Inc., the Satellite

Following the conclusion of CSRIC IV, the Commission established CSRIC V in 2016, building on the prior CSRIC's work, with its Working Group 6 specifically charged with providing "recommended capabilities to better ensure the security of the supply chain for critical communications infrastructure."[11] Working Group 6 provided guidance on these supply chain security issues in March and September 2016 reports adopted by CSRIC V that addressed the use of the Framework to address supply chain risk from suppliers.[12]

The capabilities recommended in the *March Report* "make use of security-by-design principles and processes that enable network equipment manufacturers to make the core communications network more secure, resilient, and defendable from attacks."[13] Further, the *March Report*:

> contains recommendations and best practices for communications providers that allow for the evaluation and validation of existing security-by-design processes. The recommendations are intended for use by any organization – regardless of size – that must address the integrity of the core network. In developing this report, the stakeholders provided the perspective of owners and operators of the core network; as well as that of suppliers and vendors who prioritize the incorporation of security principles into the life cycle of their products and services.[14]

Industry Association, Huawei Technologies, Inc. (USA), the American Cable Association, and NTCA – The Rural Broadband Association.

[11] CSRIC V, Working Group Descriptions and Leadership at 6 (Dec. 2016).

[12] CSRIC V, *Secure Hardware and Software: Security-By-Design Working Group 6: Final Report* (March 2016) (*March Report*); CSRIC V, *Secure Hardware and Software: Security-By-Design Working Group 6: Final Report* (September 2016) (*September Report*).

[13] *March Report* at 8.

[14] *March Report* at 5. The Working Group relied on the National Sector Risk Assessment's (NSRA's) definition of "core network," which was also relied upon in the CSRIC IV *Working Group 4 Report*. The *Working Group 4 Report* provides the following guidance regarding the core network:

> The core network transports a high volume of aggregated traffic over large distances; typically via fiber or satellite and interconnects with access networks across the country. The core network is global, connecting all continents except Antarctica using submarine fiber optic cable systems and land-based fiber and copper facility networks. The converged core network uses various technologies for the physical (layer 1) and transport layers (layer 2) for the transport of the services…Multiple service providers operating distinct core networks traversing the entire country provide the communications core infrastructure. These networks are primarily composed of wireline networks. The voice, video, and data services typically require some kind of routing translation query such as a host name look up or toll-free number query and are provided as part of operating the core network. In addition, the Network Operations Center (NOC), customer care

The *March Report* also includes a table summarizing the recommended best practices for communications sector members to use to assess and manage supply chain cybersecurity risk.[15]

Building on the *March Report's* recommended voluntary best practices for successfully incorporating security-by-design principles in the core communications network, and the iterative CSRIC process, the *September Report* examined and reviewed "the best ways to provide assurances to the FCC and the public that recommended security capabilities are being implemented by network equipment vendors, and to recommend voluntary mechanisms that provide assurances to the FCC and the public that the security practices are being applied."[16] In particular, the *September Report* stated that "security by design/supply chain risk management programs may be appropriately considered, among other topics, at yearly in-person meetings that were contemplated as part of CSRIC IV…recommendations adopted in March, 2015.[17] In addition, CSRIC recommended against "implementing any new or additional regulations to address conformity to a particular supply chain risk assessment mechanism, or any type of written attestation to the same."[18] It further stated that "in person meetings will continue to foster the public-private sector collaboration encouraged in past CSRIC reports."[19]

In seeking public comment on the CSRIC IV Report in 2015, the Bureau noted that the "detailed report" capped off "an effort by over 100 cybersecurity experts from the communications sector, federal government, state government, equipment manufacturers, cybersecurity solution providers, and the financial, banking, and energy sectors."[20] It also noted that the report, which was unanimously adopted by CSRIC IV, "includes segment-specific analysis of the application of the Cybersecurity Framework as well as recommendations in response to the Commission's charge."[21] Beyond the 2015 Public Notice seeking comment on the CSRIC IV report, and the follow-on work of CSRIC V *specifically focused on supply chain security issues and the two resulting comprehensive reports*, the Commission has taken no action on the CSRIC recommendations or the comments filed on the CSRIC IV report.

This critical, comprehensive and collaborative body of work provides the key foundation for understanding and addressing risk to the communications sector from information and communication technology products and services and the path forward for doing so. RWA urges the Commission to undertake its supply chain security efforts from this vantage point, further

> centers, and data centers for all the access networks reside on the core network…The access networks connect the end users to the core network. Traffic may originate and terminate with an access network without connecting to the core network.

[15] *March Report* at 11-17.
[16] *September Report* at A-2.
[17] *Id.* at A-10
[18] *Id.*
[19] *Id*.
[20] *CSRIC IV Report Public Notice* at 2.
[21] *Id*.

building on the work of CSRIC IV and CSRIC V, rather than abandoning those efforts in favor of a ban on specific vendors via a USF eligibility disqualification that will have the unintended consequence of harming the maintenance and advancement of broadband services in rural America, with no corresponding network security benefit.

Pursuant to Section 1.1206 of the FCC's Rules,[22] this *ex parte* is being filed electronically with the Office of the Secretary.

Respectfully submitted,

/s/ Caressa D. Bennet
Caressa D. Bennet, General Counsel
Erin P. Fitzgerald, Regulatory Counsel
5185 MacArthur Blvd., NW, Suite 729
Washington, DC 20016
(202) 857-4519
legal@ruralwireless.org

[22] 47 C.F.R. § 1.1206.