Before the
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, DC 20230

In the Matter of	)	
	)	
Promoting the Sharing of Supply Chain	)	Docket No. 200609-0154
Security Risk Information Between	)	RIN 0660-XC046
Government and Communications	)	
Providers and Suppliers	)	

COMMENTS OF T-MOBILE USA, INC.

Steve B. Sharkey
John Hunter

T-MOBILE USA, INC.
601 Pennsylvania Avenue, N.W.
Suite 800
Washington, DC 20004
(202) 654-5900

July 28, 2020

TABLE OF CONTENTS

Before the
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, DC 20230

In the Matter of	)	
	)	Docket No. 200609-0154
Promoting the Sharing of Supply Chain	)	RIN 0660-XC046
Security Risk Information Between	)	
Government and Communications	)	
Providers and Suppliers	)	

COMMENTS OF T-MOBILE USA, INC.

T-Mobile USA, Inc. ("T-Mobile")[1/] submits these comments in response to the Notice and Request for Comments issued by the National Telecommunications and Information Administration ("NTIA") in the above-referenced proceeding that requests input on ways to facilitate the sharing of security risk information with trusted providers of advanced communications services and suppliers of communications equipment.[2/] T-Mobile is committed to deploying secure fifth-generation ("5G") wireless technologies and safeguarding the integrity of the 5G supply chain. It is already actively engaged with Federal government agencies in public-private partnerships to evaluate, share information about, and address security threats. NTIA should leverage the experience of these existing structures as it develops its program to share supply chain security risk information, particularly with small and rural providers, and take

---

1/ T-Mobile USA, Inc. is a wholly-owned subsidiary of T-Mobile US, Inc., a publicly traded company. T-Mobile and Sprint are now one company operating under the name T-Mobile. The merger closed on April 1, 2020.

2/ *See Promoting the Sharing of Supply Chain Security Risk Information Between Government and Communications Providers and Suppliers*, Notice; Request for Public Comment, 85 Fed. Reg. 35,919 (June 12, 2020) ("*Request for Comments*"); *Promoting the Sharing of Supply Chain Security Risk Information Between Government and Communications Providers and Suppliers*, Notice; Extension of Comment Period, 85 Fed. Reg. 40,625 (July 7, 2020) (extending the comment deadline to July 28, 2020); *see also* Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 134 Stat. 158 (2020) ("Secure and Trusted Communications Networks Act").

other targeted steps to protect the Nation's communications infrastructure from potential security threats.

I. INTRODUCTION AND SUMMARY

As U.S. communications service providers increasingly rely on a diverse ecosystem of equipment, including some manufactured by foreign companies, the Nation faces new challenges to ensure the security of the telecommunications supply chain. The Secure and Trusted Communications Networks Act of 2019 (the "Act") seeks to address those challenges by, among other things, directing NTIA, in coordination with other Federal agencies, to establish a program to share supply chain security risk information – through "regular briefings and other events" – with trusted providers of advanced communications services and suppliers of communications equipment or services.[3/] The Act also requires NTIA to "engage with" trusted providers and suppliers, particularly those providers and suppliers that are small businesses or primarily serve rural areas.[4/]

T-Mobile supports the Act's goal of, among other things, facilitating the sharing of supply chain security risk information. Indeed, T-Mobile already participates in many activities envisioned by the Act and engages in public-private partnerships with government entities to share critical information. For example, T-Mobile is a member of both the National Coordinating Center for Communications ("NCC") and the Information and Communications Technology ("ICT") Supply Chain Risk Management ("SCRM") Task Force established by the Department of Homeland Security's ("DHS") Cybersecurity & Infrastructure Security Agency

3/ *See* Secure and Trusted Communications Networks Act, 134 Stat. at 168.

4/ *See id.*

("CISA").[5/] In addition, T-Mobile is a member of the Communications Sector Coordinating Council ("CSCC"),[6/] which works with government partners to protect the Nation's communications critical infrastructure and key resources from harm and ensure that the Nation's communications networks and systems are secure, resilient, and rapidly restored after a natural or manmade disaster.[7/] T-Mobile also participates in the Network Security Information Exchange established by the National Security Telecommunications Advisory Committee, an information-sharing forum charged with devising strategies for mitigating cyber threats to the public network,[8/] and is a member of the Alliance for Telecommunications Industry Solutions, which includes a 5G Supply Chain Working Group that works with the Department of Defense and other Federal agencies to create supply chain standards for trusted 5G networks that can be operationalized in the public and private sectors.[9/]

While other industry members also participate in these activities, some smaller and rural entities, as the Act acknowledges,[10/] may not have access to the information they need to

---

5/ *See* Department of Homeland Security, Cybersecurity & Infrastructure Security Agency, The National Coordinating Center for Communications (NCC), https://us-cert.cisa.gov/nccic/ncc-watch (last visited July 21, 2020) ("NCC Website"); Department of Homeland Security, Cybersecurity & Infrastructure Security Agency, Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force ("ICT SCRM Task Force Website"), https://www.cisa.gov/ict-scrm-task-force (last visited July 21, 2020).

6/ *See* NCC Website; ICT SCRM Task Force Website.

7/ *See* US Communications Sector Coordinating Council, Membership, https://www.comms-scc.org/members (last visited July 21, 2020); US Communications Sector Coordinating Council, Mission of the C-SCC, https://www.comms-scc.org/mission (last visited July 21, 2020).

8/ *See* National Security Telecommunications Advisory Committee, *Network Security Information Exchange Fact Sheet*, https://www.cisa.gov/sites/default/files/publications/NSIE%20Factsheet%20%2808 2019%29-%20508%20compliant.pdf (last revised Oct. 2019).

9/ *See* ATIS, Membership, https://www.atis.org/01_membership/members/ (last visited July 21, 2020); ATIS, 5G Supply Chain Working Group, https://www.atis.org/01_strat_init/5g-supply-chain/ (last visited July 21, 2020).

10/ *See* Secure and Trusted Communications Networks Act, 134 Stat. at 168.

recognize that certain providers and suppliers pose a security risk. As Congress has noted, although "[l]arge communications companies with sophisticated network security operations and significant capital generally have avoided installing and using Huawei and other suspect foreign equipment in their networks . . . some smaller carriers with more limited resources and less sophisticated security operations have purchased and installed Huawei, and other suspect foreign equipment, in their networks either because the equipment was less expensive or they were unaware of the security risk, or both."[11/]

The program that NTIA will develop will help address these gaps in supply chain information and mitigate against security threats. Government dissemination of information to which industry may not have access will not only facilitate the identification of existing threats, but also help detect future threats and prevent their introduction into U.S. communications networks and the supply chain. To create a successful program, NTIA should take full advantage of existing structures and maintain consistency across defined terms and implementation of the program. And while the Act's focus is on sharing supply chain security risk data with small and rural entities, NTIA should broadly interpret the types of information it is obligated to share. Finally, NTIA should ensure that the information is easily accessible, including through expedited security clearance procedures, and that any information that can be made available is, in fact, made available to *all* trusted providers and suppliers.

[11/] H. Rept. 116-352, Secure and Trusted Communications Networks Act of 2019, at 9 (Dec. 16, 2019) ("House Report"), https://www.congress.gov/116/crpt/hrpt352/CRPT-116hrpt352.pdf. Indeed, the Rural Wireless Association acknowledges that one quarter of its membership likely uses equipment from suppliers like Huawei and ZTE. *See* Oliver McPherson-Smith and Steve Pociask, *Huawei is Embedded in Our Infrastructure and the Federal Government Subsidized It*, THE HILL (Aug. 21, 2019), https://thehill.com/blogs/congress-blog/technology/458260-huawei-is-embedded-in-our-infrastructure-and-the-federal; Reply Comments of the Rural Wireless Association, WC Docket No. 18-89, at 15 (filed Dec. 7, 2018).

II. NTIA SHOULD TAKE MAXIMUM ADVANTAGE OF EXISTING INFORMATION SHARING ORGANIZATIONS AND PROGRAMS

As NTIA recognizes, important work is already being performed with respect to supply chain security risks. For example, it notes that there are existing threat and vulnerability information sharing programs and that the Federal Acquisition Security Council established by the Federal Acquisition Supply Chain Security Act of 2018 (the "FASC") is already developing risk information sharing policies that are "comparable to those that the Act contemplates" and will inform NTIA's program.[12/] NTIA has also moved quickly to establish the Communications Supply Chain Risk Information Partnership to support its program, which will be implemented in phases and is aimed at improving access by trusted small and rural communications providers and equipment suppliers to risk information about key elements in their supply chain.[13/]

The public-private partnerships noted above in which T-Mobile is actively engaged similarly assess and work to address security risks. The NCC, for example, continuously monitors national and international incidents and events that may impact emergency communications, including cybersecurity threats.[14/] Federal agencies like the Department of Commerce and the FCC also play an important role in the NCC, working with private industry to facilitate the exchange of vulnerability, threat, instruction, and anomaly information that are critical to the sustainment of national security and emergency preparedness communications. Additionally, the ICT SCRM Task Force – the Nation's preeminent public-private supply chain

---

12/ *See Request for Comments* at 35,920-21.

13/ *See Establishment of the Communications Supply Chain Risk Information Partnership*, Notice, 85 Fed. Reg. 41,006 (July 8, 2020).

14/ *See* NCC Website.

risk management partnership – has been entrusted with the critical mission of identifying and developing consensus strategies to enhance ICT supply chain security.[15/]

The Act states that the program that NTIA establishes should be "integrated with, ongoing activities of the Department of Homeland Security and the Department of Commerce."[16/] T-Mobile agrees. Accordingly, NTIA should incorporate the activities discussed above into its mandate to "conduct regular briefings and other events" and "engage with trusted providers" and ensure that access to information through its program is consistent with existing Federal government initiatives.

III. NTIA SHOULD BROADLY INTERPRET THE TYPES OF INFORMATION THAT SHOULD BE SHARED

NTIA seeks input on the definition of several terms to determine the types of information it should share.[17/] To the extent there are already existing government formulations of certain terms, NTIA should rely on those existing definitions in order to maintain consistency across Federal activities. For example, as NTIA points out, "supply chain risk" is already defined by the FASC.[18/] T-Mobile supports the use of that definition as well as relying on the designations in Section 2(c)(1-4) of the Act for the definition of "trusted providers and suppliers."[19/] Moreover, T-Mobile supports NTIA's reliance on the Act's definition of "foreign adversary," which is identical to that in the President's Executive Order on Securing the Information and

---

15/ *See* ICT SCRM Task Force Website.

16/ Secure and Trusted Communications Networks Act, 134 Stat. at 168.

17/ *See Request for Comments* at 35,920-21.

18/ *See id.* at 35,920.

19/ *See id.* at 35,920-21; Secure and Trusted Communications Networks Act, 134 Stat. at 158-59.

Communications Technology and Services Supply Chain (E.O. 13873).[20/] As NTIA observes, relying on other relevant Federal determinations will "ensure consistency of action across the Federal government."[21/] And if those definitions are changed by the expert government agencies, NTIA can, and should, modify its characterizations as appropriate to avoid creating discrepancies between the activities of other agencies.

NTIA, however, should not unnecessarily limit its interpretation or definition of "supply chain security risk information" with respect to the types of information that will be shared with trusted providers and suppliers. Providers and suppliers need access to as much information as possible to make informed decisions – having access to some information will always be better than having access to none. NTIA should therefore facilitate the release of the maximum amount of information to program participants.

IV. NTIA SHOULD CREATE EASILY IDENTIFIABLE SOURCES OF, AND A STREAMLINED PROCESS FOR OBTAINING, INFORMATION

NTIA requests comment on the best means for sharing information and ways for the Federal government to provide "regular briefings."[22/] Congress has explained that the purpose of the Act and the program is to mitigate threats posed in vulnerable communications equipment and services and to assist small communications providers with the costs of removing and replacing equipment and services that pose a threat from their networks.[23/] The purpose of the

---

20/ *See Request for Comments* at 35,921; *Executive Order 13873, Securing the Information and Communications Technology and Services Supply Chain*, 84 Fed. Reg. 22,689 (May 17, 2020).

21/ *Request for Comments* at 35,921.

22/ *See id*.

23/ *See* House Report at 8-9; *see also Request for Comments* at 35,921 (adding that "Congress deemed reimbursement for such entities appropriate because it believed that smaller providers did not receive a sufficient 'heads-up by our government' about the security risks posed by certain equipment and services . . . ").

Act, however, will be defeated if there are multiple sources of threat information and providers are unsure which source provides the most credible and useful information about a threat.

Because, as noted above, DHS is already sharing much of the information contemplated by the Act with the private sector, NTIA's program should feature DHS' CISA as the primary source of the "regular briefings" NTIA is required to provide. CISA routinely provides alerts about current security issues, vulnerabilities, and exploits as well as more in-depth reports and analyses on new or evolving threats.[24/] And it offers a variety of information to users with varied technical expertise.[25/] Indeed, the ICT SCRM Task Force under CISA, of which NTIA is a member, specifically includes a working group that is dedicated to the timely sharing of actionable information about supply chain risks across the community.[26/]

Providing information through DHS will also engage the protections of CISA. For example, DHS maintains a Private Sector Clearance Program for Critical Infrastructure that ensures critical infrastructure private sector owners, operators, and industry representatives receive the security clearances they need to access classified information and make more informed decisions.[27/] CISA's enacting statute – the Cybersecurity and Infrastructure Security

---

[24/] *See* Department of Homeland Security, Cybersecurity & Infrastructure Security Agency, National Cyber Awareness System, https://us-cert.cisa.gov/ncas (last visited July 21, 2020).

[25/] *See id.* (explaining that "[t]hose with more technical interest can read the Alerts, Analysis Reports, Current Activity, or Bulletins" and "[u]sers looking for more general-interest pieces can read the Tips").

[26/] *See* Department of Homeland Security, Cybersecurity & Infrastructure Security Agency, *Information and Communications Technology Supply Chain Risk Management Task Force: Interim Report*, at iv (Sept. 2019), https://www.cisa.gov/sites/default/files/publications/ICT%20Supply%20Chain%20Risk%20Management%20Task%20Force%20Interim%20Report%20%28FINAL%29_508.pdf.

[27/] *See* Department of Homeland Security, *Privacy Impact Assessment Update for the Private Sector Security Clearance Program for Critical Infrastructure*, DHS/NPPD/PIA-020(b) (Apr. 20, 2018), https://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-020%28b%29-pscp-april2018.pdf; Department of Homeland Security, *Privacy Impact Assessment Update for the Private Sector Security*

Agency Act of 2018 – further requires that any materials received by CISA "is protected from unauthorized disclosure and handled and used only for the performance of official duties."[28/] Thus, both private and public sector program participants can be assured that information sent to and from DHS and CISA would remain secure.

Providers and suppliers also need *timely* access to information. Without timely access to information, providers and supplies will be unable to take preventative actions; they will only be able to remediate. If affording timely access means allowing trusted providers and suppliers to receive certain non-classified information first because classified information takes time to redact, then that non-classified information should be made available first.

To the extent trusted providers and suppliers are subject to security clearance requirements to participate in NTIA's program, they should be permitted to do so from an identified single source and be afforded an expeditious process for granting clearance. NTIA should therefore examine how security clearances can be provided to trusted vendors for the limited purposes of receiving or requesting security risk information. NTIA could, for example, leverage DHS' experience with its Private Sector Clearance Program, including by providing periodic updates to its security clearance procedures and expediting the process where possible and appropriate.[29/] At a minimum, NTIA should evaluate mechanisms to streamline security

---

Clearance Program for Critical Infrastructure, DHS/NPPD/PIA-020(a) (Feb. 11, 2015), https://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-pscp-february2015.pdf ("DHS 2015 Update").

[28/] Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115-278, 132 Stat. 4168, 4172 (2018); *see also* Department of Homeland Security, Cybersecurity & Infrastructure Security Agency, About Us, https://us-cert.cisa.gov/about-us (last visited July 21, 2020) ("As a global information exchange hub, CISA bears a significant responsibility to protect the information we receive and to ensure we safeguard privacy, business confidentiality, civil rights, and civil liberties.").

[29/] *See, e.g.*, DHS 2015 Update at 2 (explaining that DHS was updating its security clearance program consistent with Executive Order 13636, which directed DHS to "expedite the processing of security clearances to appropriate personnel employed by critical infrastructure owners . . .").

clearances for the limited purposes of trusted providers and suppliers receiving vital, but classified, material regarding security risks. It should further develop means by which small and rural entities – who are not routinely engaged in obtaining security clearances – can obtain clearance as soon as possible and with limited administrative burdens.

V. NTIA SHOULD DISCLOSE INFORMATION WIDELY WITH SPECIAL OUTREACH TO SMALL AND RURAL PROVIDERS

NTIA asks if there are other factors aligned with the Act that should be considered in determining "trusted" providers and suppliers eligible for the program.[30/] In addition to interpreting the terms of the Act broadly to foster information sharing, NTIA should facilitate the release of information to the broadest group of program participants. Although the Act limits the reimbursement of funds for removing, replacing, and disposing of communications equipment or services that pose an unacceptable risk to national security to small and rural entities,[31/] that does not mean only those entities need access to security risk information. The purpose of the Act is for the government to provide information to trusted providers and suppliers, particularly small and rural entities, to prevent security risks. But *all* trusted providers and suppliers need information to secure the supply chain because they all impact the national wireless ecosystem. Accordingly, the Act will have the most meaningful impact if "trusted" providers and suppliers is broadly interpreted.

But NTIA should take special care to ensure that small and rural entities are fully informed about potential threats and mechanisms for removing and replacing services and

---

30/ *See Request for Comments* at 35,921.

31/ *See* Secure and Trusted Communications Networks Act, 134 Stat. at 160-66.

equipment that pose a threat. As Congress recognized and recent events have made clear,[32/] small and rural entities are particularly vulnerable to security risks posed by vendors that may under-price products in order to secure access to U.S. networks. While T-Mobile has always focused on implementing secure networks with trusted vendors, small and rural providers may focus heavily on pricing. And those risks impact everyone in the mobile wireless marketplace. That is why those same small and rural vendors must now replace equipment deemed to be a security risk.[33/] For the broadest impact, NTIA should reach small and rural providers by issuing bulletins on its website and by ensuring that it provides the same information to sources such as trade associations, the Small Business Administration, and other similar outlets. Those sources are not only specifically organized to provide assistance to small and rural entities,[34/] but small and rural entities are also familiar with, and more likely to utilize, them.

NTIA should also encourage small and rural entities to become members of the National Cybersecurity and Communications Integration Center ("NCCIC").[35/] Not only does the NCCIC

32/ *See* House Report at 9; *see also* Todd Shield, *FCC Calls Huawei, ZTE Security Threats as It Bars Subsidies*, BLOOMBERG (June 30, 2020), https://www.bloomberg.com/news/articles/2020-06-30/fcc-designates-china-s-huawei-zte-as-national-security-threats ("The U.S. Federal Communications Commission designated Huawei Technologies Co. and ZTE Corp. as national security threats, a step toward driving the Chinese manufacturers from the U.S. market where small rural carriers rely on their cheap network equipment.").

33/ *See* Secure and Trusted Communications Networks Act, 134 Stat. at 160-66.

34/ *See, e.g.*, U.S. Small Business Administration, About SBA, https://www.sba.gov/about-sba (last visited July 21, 2020) ("The SBA is the only cabinet-level federal agency fully dedicated to small business and provides counseling, capital, and contracting expertise as the nation's only go-to resource and voice for small businesses."); Rural Wireless Association, About Us, https://ruralwireless.org/about-rwa/ (last visited July 21, 2020) ("RWA's mission is to promote wireless opportunities for rural telecommunications companies through advocacy and education in a manner that best represents the interests of its membership.").

35/ *See* Department of Homeland Security, Cybersecurity & Infrastructure Security Agency, National Cybersecurity and Communications Integration Center, https://us-cert.cisa.gov/nccic?__hstc=245485531.267f74747c9821ec26a48120809aad7e.1486339200049.1486339200051.1486339200052.2&__hssc=245485531.1.1486339200052&__hsfp=528229161 (last visited July 21, 2020) (explaining that the NCCIC is comprised of four branches, including the NCC, and "serves as a central location where a diverse set of

provide a range of services to private industry related to network protection and information sharing,[36/] but membership in the NCCIC would also be an ideal means by which NTIA could identify the appropriate points of contact at small and rural businesses. That information is already required for applications to participate in the Communications Information Sharing and Analysis Center of the NCC – a branch of the NCCIC – and thus could be used for NTIA's program without requiring small and rural entities to provide duplicative information.

VI. CONCLUSION

T-Mobile appreciates and supports NTIA's efforts to establish a program to share supply chain security risk information with trusted providers and suppliers, particularly small and rural entities. Because the increasingly globalized market for equipment and services has opened the door for potentially threatening goods and services from foreign adversaries, it is critical that the wireless industry work together to mitigate against these security risks. To maximize its potential and effectiveness, NTIA should base its program on existing government initiatives and partnerships, have a broad focus, and feature outreach to representatives of small and rural providers.

---

partners involved in cybersecurity and communications protection coordinate and synchronize their efforts"). As with all of the activities outlined above in which small and rural providers should be encouraged to participate, the trade associations to which those entities belong should also be encouraged to participate in the NCCIC. Small and rural carriers may not have the resources to fully engage in the government and public-private partnerships noted, but their trade associations may be better positioned to do so and transmit information to members.

36/ *See* Department of Homeland Security, *NCCIC Services for Private Industry*, https://us-cert.cisa.gov/sites/default/files/documents/NCCIC%20Service%20Menu%20-%20Private%20Industry.pdf.

Respectfully submitted,

/s/ *Steve B. Sharkey*
Steve B. Sharkey
John Hunter

T-MOBILE USA, INC.
601 Pennsylvania Avenue, N.W.
Suite 800
Washington, DC 20004
(202) 654-5900

July 28, 2020