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

COMMENTS OF AT&T SERVICES, INC.

AT&T Services, Inc., on behalf of its affiliates, ("AT&T") submits these comments on the Notice of Proposed Rulemaking in the above proceeding.[1]

AT&T's network infrastructure is the core asset over which AT&T provides an array of advanced communications services to many millions of customers in the U.S. and elsewhere ranging from the largest global businesses to individual consumers. AT&T is strongly committed to ensuring effective network security and uses a range of procedures and practices to protect its customers, network, and services.[2]

---

[1] *Notice of Proposed Rulemaking*, WC Docket No. 18-89, FCC 18-42, Apr. 18, 2018 ("*Notice*"). The Notice proposes to prohibit the use of universal service support to purchase or obtain any equipment or services produced or provided by any company posing a national security threat to the integrity of communications networks or the communications supply chain.

[2] These include continuously monitoring network traffic to identify malicious behavior and respond to vulnerabilities and attacks, using proactive and reactive defense techniques to ensure the network is as secure as possible, educating users on preventing and detecting cyber threats, and providing users with security services and tools. AT&T also participates in or coordinates with many partnerships with government entities, including the National Security Telecommunications Advisory Committee (NSTAC), the DHS National Cybersecurity and Communications Integration Center (NCCIC), the U.S. Secret Service (USSS) Cyber Crimes Task Force, the Federal Bureau of Investigation's InfraGard®, the Network Reliability and Interoperability Council (NRIC), the Communications Security, Reliability and Interoperability Council (CSRIC), the Communications Sector Coordinating Council (CSCC) and the Communications Information Sharing and Analysis Center (Comms-ISAC). Additionally, the

(Footnote continued on next page)

In these comments, we focus on the importance of ensuring that national security concerns are addressed in an effective, nondiscriminatory manner that minimizes unintended consequences. As described below, any measures to address legitimate national security threats should be proportionate to the security risks and apply equally to *all* networks and providers without regard to technology or size, and not just to entities that use Universal Service Fund (USF) support or that are otherwise subject to the Commission's regulatory authority.

1. National Security-Related Restrictions Should Apply to All Operators Regardless of Regulatory Classification

Communications networks operated by telecommunications carriers, cable companies and technology companies all provide voice, data and video services in today's converged U.S. telecommunications and information market. These networks support the Internet, electronic commerce, the Internet of Things ("IoT") and other advanced communications services critical to our economy and society. In particular, technology and cable companies are important providers of an increasing number of these services.

For example, technology companies not only provide highly popular voice and messaging services used by hundreds of millions of users throughout the world but also compete to serve business customers in high growth areas such as cloud services.[3] As cloud computing is

(Footnote continued from previous page)

AT&T Security Research Center conducts research on a variety of security issues. *See* https://src.att.com/index.html.

[3] *See AWS vs Azure vs Google Cloud Market Shares 2017* (reporting that Amazon, Microsoft, and Google are the leading providers of public cloud services), https://www.google.com/search?ei=qPTxWsihMYfwzgLwra4w&q=azure+vs+aws+2017&oq=azure+vs+aws&gs_l=psy-ab.1.0.0i71k1l8.0.0.0.36175.0.0.0.0.0.0.0.0..0.0....0...1c..64.psy-ab..0.0.0....0.s3ykjxmKpD0. *See also, Facebook and Microsoft are Laying a Giant Cable Across the Atlantic*, May 26, 2016 ("Rather than just leasing bandwidth on undersea cables and

(Footnote continued on next page)

increasingly used as an underlying technology for IoT services to connect and manage devices and store and process data, cloud providers play an important role in protecting the security of IoT services.[4] Even without considering potential national security threats to underlying network equipment, both the GAO and the FTC Staff have underscored the importance of protecting the security of customers and networks in connection with the growth of the IoT.[5]

To effectively protect the communications supply chains that serve this converged marketplace against national security threats, restrictions to address such threats should apply to all U.S. telecom and information network operators. A competitively-neutral and nondiscriminatory approach is also required to avoid impeding the continuing vitality of the competitive U.S. telecom and information marketplace. With providers' choices of equipment and services strongly impacting both cost and innovation, restricting the equipment and service choices of some market participants but not others, as would result from limiting such measures to USF recipients, would potentially distort competition and harm consumers.

(Footnote continued from previous page)

terrestrial connections operated by telecoms, the likes of Google, Facebook, and Microsoft are building their own networking infrastructure on both land and across seas."), https://www.wired.com/2016/05/facebook-microsoft-laying-giant-cable-across-atlantic/?mbid=email_onsiteshare; *Three New Submarine Cables to Link Google Cloud Data Centers*, Jan. 17, 2018, http://www.datacenterknowledge.com/google-alphabet/three-new-submarine-cables-link-google-cloud-data-centers.

[4] *See, e.g.*, *Why Cloud Computing is the Foundation of the Internet of Things*, Feb. 15, 2017, https://www.thorntech.com/2017/02/cloud-computing-foundation-internet-things/.

[5] *See* U.S. Government Accountability Office, *Internet of Things, Status and Implications of an Increasingly Interconnected World*, May 2017; FTC Staff Report, *Internet of Things, Privacy and Security in a Connected World*, Jan. 2015.

The Notice identifies no clear authority that would allow the Commission to address national security threats to the communications supply chain outside the USF context, and in today's highly competitive environment, restrictions and regulations that apply only to a subset of the industry threaten to do more harm than good.

2. Restrictions Also Should be Proportionate to Legitimate Security Risks

In addressing these issues, policymakers also should seek to preserve as much as possible the significant benefits U.S. consumers and businesses receive from U.S. operators' global equipment supply chains and global communications networks by framing protective measures to be proportionate to legitimate security risks. Since the U.S. is viewed as a global leader in telecommunications regulatory matters, other countries are likely to pay close attention to how the U.S. addresses these issues and could seek to use U.S. restrictions as precedent to justify overbroad foreign restrictions. While any U.S. restrictions, however narrowly framed, could potentially be used to justify overbroad foreign restrictions that would harm U.S. interests, U.S. restrictions that are clearly proportionate to legitimate U.S. security interests are less likely to provoke such retaliation.

The hardware and software products used by U.S. operators now include a diverse mix of inputs from the U.S. and its trading partners that provide major U.S. consumer benefits.[6] Significant benefits also result from the services AT&T and other U.S. network operators provide to U.S. and foreign customers throughout the world by obtaining foreign licenses and

[6] *See, e.g.*, T.H. Moran & L. Oldenski, *How Offshoring and Global Supply Chains Enhance the U.S. Economy*, Institute for International Economics, Apr. 2016, at 3, https://piie.com/publications/policy-briefs/how-offshoring-and-global-supply-chains-enhance-us-economy; R. D. Atkinson & L.A. Stewart. ITIF, *Just the Facts: The Economic Benefits of Information and Communications Technology* (2013).

building networks in foreign markets or by cooperating with foreign operators for "last mile" and similar services. These services allow U.S. businesses to communicate seamlessly throughout the world both within their organizations and with their customers, thus increasing the efficiency of their operations and earning greater revenues in foreign markets. By ensuring that security measures are fact-based and proportionate to legitimate security threats, U.S. policymakers would reduce the possibility of U.S. restrictions leading to the exclusion of U.S. telecommunications and information products and services from foreign markets based on unsupported security claims, or unnecessarily depriving U.S. consumers and businesses of the benefits of global supply chains.

To protect further against U.S. security measures being perceived as illegitimate, they should not be modified based on unrelated policy priorities. Since a legitimate national security interest should not be susceptible to any such modification, allowing national security restrictions to be modified based on impacts on policies assisting smaller operators or promoting network deployment, as suggested by the Notice,[7] would likely undermine their legitimacy and raise the risk of retaliation that would harm U.S. consumers and businesses. Similarly, allowing upgrades of existing equipment obtained from restricted suppliers, or grandfathering existing contracts with such suppliers, would weaken the legitimacy of adopted measures by perpetuating the underlying security risk, as well as continuing any associated cost or capability benefits of such equipment to the disadvantage of competing operators.[8]

---

[7] *See* Notice, ¶¶ 33-34.

[8] Additionally, the potential treatment of mobile devices under the proposed rule should be clarified. Any application of the proposed rule to mobile devices should require evidence of potential harm to wireless or wireline networks resulting from the use of mobile devices. In the

(Footnote continued on next page)

In conclusion, to provide effective security and avoid adverse impacts to the competitive U.S. marketplace and U.S. interests in foreign markets, legitimate national security threats should be addressed by proportionate measures applied to all operators of U.S. wireline and wireless telecommunications and information networks on a competitively-neutral, nondiscriminatory basis.

Respectfully submitted,

By: /s/ James Talbot

James J. R. Talbot
Gary L. Phillips
David L. Lawson

Attorneys for
AT&T SERVICES, INC.
1120 20th Street, NW
Washington, D.C. 20036
(202) 457-3048

Dated: June 1, 2018.

(Footnote continued from previous page)

absence of such evidence, restrictions on the purchase or use of devices may be viewed as overbroad and also could lead to foreign restrictions that would harm U.S. interests.