Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

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

To: The Commission

COMMENTS OF ECHOSTAR SATELLITE OPERATING CORPORATION AND HUGHES NETWORK SYSTEMS, LLC

Jennifer A. Manner
Senior Vice President
Regulatory Affairs

Paul Kay
Chief Information Security Officer

EchoStar Satellite Operating Corporation
Hughes Network Systems, LLC
11717 Exploration Lane
Germantown, MD 20876

June 1, 2018

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

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

To: The Commission

COMMENTS OF ECHOSTAR SATELLITE OPERATING CORPORATION AND HUGHES NETWORK SYSTEMS, LLC

EchoStar Satellite Operating Corporation and Hughes Network Systems, LLC (collectively, "EchoStar") submit these comments in response to the Commission's Notice of Proposed Rulemaking seeking comment on issues related to protecting the security of America's communications networks against threats related to the supply chain.[1] As discussed in more detail below, EchoStar supports the Federal Communications Commission's ("FCC's") actions to ensure that Universal Service Fund ("USF") support is not used to purchase equipment or services produced or provided by a company posing a national security threat to the integrity of communications networks or the communications supply chain. The rule should be easy for USF recipients and other stakeholders to administer – for example, it should not require support recipients to inquire into the provenance of the components making up equipment that is manufactured by a company that is not on the suspect list. Further, lists of problematic manufacturers should derive from broader policy processes that advance industry-driven principles of cybersecurity and supply chain risk management.

[1] *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Notice of Proposed Rulemaking, FCC 18-42 (rel. April 18, 2018) ("NPRM").

I. SUPPLY CHAIN SECURITY IS A CRITICAL ELEMENT OF ECHOSTAR'S BROADER NETWORK SECURITY EFFORTS

EchoStar Corporation ("EchoStar"), a Denver based company, is the largest U.S. commercial geostationary orbit ("GSO") satellite operator and the fourth-largest GSO operator worldwide. Through its subsidiaries, EchoStar Satellite Services and Hughes Network Systems, LLC, EchoStar provides broadband, video, and other services to meet the needs of small and large customers, including media and broadcast organizations, direct-to-home ("DTH") providers, enterprise customers, government service providers, and residential consumers in North America and globally.

Hughes provides high speed broadband services across the Americas, and recently brought into service the EchoStar XIX/Jupiter 2 satellite in December 2016. With the addition of Jupiter 2, Hughes launched its new HughesNet Gen5 satellite Internet service; delivering faster speeds (meeting FCC broadband definitions), more data, and built-in Wi-Fi for consumers and small businesses across the continental United States, Southeastern Alaska, Puerto Rico, the U.S. Virgin Islands, Mexico, Canada, Brazil, and Colombia.

Since launching the HughesNet Gen5 service in March 2017, almost half of Hughes' 1.2 million consumers in North America and Brazil receive the new service. Gen5 provides consumers with Commission-defined broadband speeds of 25 Mbps down 3 Mbps up, with no hard data caps and installation within days. HughesNet customers have been so satisfied with the new service that Hughes has experienced four consecutive quarters of decreased retail churn since the launch of Gen5. Per the Commission's recent public notice, Hughes has submitted a short-form application to participate in the Connect America Fund Phase II auction (Auction 903).[2]

In addition to its satellite services, Hughes develops innovative equipment for the world's communications markets and manufactures equipment at two facilities in in the United States. Hughes pioneered the development of very small aperture terminals ("VSATs") and remains the world's leading provider of enterprise VSAT services. Hughes also designs and develops a wide range of mobile satellite and broadband equipment,

As a result of Hughes' global leadership in the development of satellite solutions, Worldvu Satellites Limited d/b/a OneWeb selected Hughes to develop its ground system, including gateways and user terminals, for its global low earth orbit ("LEO") satellite constellation. The joint development of the ground network, currently valued at over $300 million, began in 2015 and shipments are expected to begin in mid-2018.[3] These components are also being manufactured and assembled at the Hughes facilities in Maryland.

Hughes has recently received its Commission authorization to construct, launch, and operate its next-generation, Ultra High Density Satellite, the EchoStar XXIV/Jupiter 3. Jupiter 3 is planned for launch in early 2021 and is being manufactured by Space Systems Loral in California, with its ground network being constructed by Hughes and its partners. The Jupiter 3 satellite will be used to provide state-of-the-art satellite broadband services and capacity to customers throughout the continental United States at speeds of approximately 100 Mbps.

[2] *Connect America Fund Phase II Auction: Status of Short-Form Applications to Participate in Auction 903; Corrections Due June 5, 2018*, Public Notice, DA 18-484 (rel. May 14, 2018).

[3] *See* Hughes Network Systems, LLC, Press Release: Hughes Announces Partnership in OneWeb's Innovative Global Satellite Broadband Initiative to Close the Digital Divide, PR Newswire, 25 June 2015.; *see also* Hughes Network Systems, LLC, Press Release: Hughes Signs $190M Contract with OneWeb for Production of Ground Network System for Global Internet Services, 7 November 2017

Cybersecurity is an integral part of EchoStar's – and the satellite industry's – central role in providing mission critical, highly reliable, secure connectivity. Likewise, supply chain security is a critical component of cybersecurity. EchoStar strongly supports supply chain security policies as a means of safeguarding the nation's critical communications infrastructure, including the steps the FCC is taking in this proceeding. EchoStar has helped lead the satellite industry's efforts to provide secure solutions to diverse global customers, including military and government users, corporations of every size and type, the non-profit and scientific communities, and individual consumers. Among other initiatives, EchoStar actively participated in the development of ground-breaking recommendations to the Commission regarding cybersecurity risk reduction in the communications sector and satellite subsector under the fourth Communications Security, Reliability, and Interoperability Council (CSRIC) in 2015.[4] In addition, EchoStar helped develop the satellite industry's principles to address cybersecurity and supply chain security, the Joint Statement on the Satellite Industry's Commitment to Cybersecurity.[5] The overarching goals of these industry principles align with the focus of this proceeding, and a number of the principles are specifically relevant to the Commission's focus here. For example, the satellite industry's recommendations include:

- Recognizing that trustworthy service offerings depend on trustworthy infrastructure components and practices as well as reliable partners. Security and risk management should be considered throughout the service delivery chain from network, hardware and software design, vendor management, and customer interfaces.

[4] *See* CSRIC IV, Cybersecurity Risk Management and Best Practices, CSRIC IV, Working Group 4 Final Report (Mar. 2015), *available at* https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

[5] *See Joint Statement on the Satellite Industry's Commitment to Cybersecurity*, available at https://gvf.org/images/pdf/SIAGVFESOAcybersecMay2018.pdf.

- Equipment vendors should consider security management practices and their technical implementation on an iterative basis;
- Organizations should recognize that they can receive information about vulnerabilities from diverse internal and external sources, and should take appropriate action.

EchoStar recognizes that the government – including the FCC – has an important role on these issues, particularly in encouraging private sector leadership and government-industry collaborative partnerships. Consistent with the satellite industry principles, cybersecurity and supply chain security initiatives are most effective when they harness market drivers and empower satellite providers, resellers, software providers and equipment manufacturers to implement the security measures that work best for their particular security needs and preferences. Solutions should be flexible to adapt to ever-changing threats, so in most cases prescriptive regulatory mandates actually stifle the innovation that is needed to keep pace with the threats. As discussed below in Section III, even mandatory requirements such as those that may arise from this proceeding should be developed through processes that promote these principles.

II. PROHIBITIONS SHOULD BE CLEAR AND ADMINISTRATIVELY FEASIBLE FOR SERVICE PROVIDERS TO IMPLEMENT

Given the complexity of the communications supply chain and the products that comprise it, rules adopted in this proceeding must be clear and straightforward to enable providers to comply with them and the Commission to enforce them. The NPRM proposes to adopt a rule providing that “no USF support may be used to purchase or obtain any equipment or services produced or provided by a company posing a national security threat to the integrity of communications networks or the communications supply chain."[6] To implement this prohibition, the FCC seeks comment on whether it should: (1) adopt a broad and "bright-line approach" under which it "prohibit[s] use of USF funds on any purchases whatsoever from companies that have been identified as raising national security risks"; or, instead, (2) focus the proposed rule's prohibitions more narrowly on "equipment and services that relate to the management of a network, data about the management of a network, or any system the compromise or failure of which could disrupt the confidentiality, availability, or integrity of a network."[7]

Either of these two approaches are acceptable, but whichever approach the Commission takes, EchoStar urges the Commission to formulate the rule such that the prohibition applies to complete pieces of hardware or software. For example, the Commission could specify that recipients may not use USF support to purchase any product or service from a particular company, or that recipients may not use USF support to purchase a particular product produced by a particular company (for example, identifying the product by its model name, SKU, or both).

The Commission should *not*, however, adopt a rule that would apply to *components* or *sub-parts* of a finished product. For example, the Commission should *not* adopt a rule prohibiting recipients from using USF support to purchase any product that *may contain components manufactured by* a particular company. Purchasers of telecommunications equipment have limited visibility into all of the components that are used by their suppliers in producing particular products. Thus, if a product is produced by one company, but contains components produced by a different company (which may be on the Commission's list of

[6] NPRM at ¶ 13.

[7] *Id.* at ¶ 15.

prohibited producers), a USF recipient purchasing that product is unlikely to have the ability to know that the product contains components from a prohibited manufacturer.

Therefore, the Commission's rule should either: (1) make clear that the ban on particular manufacturers applies at the finished product level and does not require USF recipients to determine whether a product contains components produced by a different, banned manufacturer; or (2) provide USF recipients with access to a list of specific pieces of equipment (by model name, SKU, or both) that may not be purchased with USF funds because they contain components produced by forbidden manufacturers.[8] Either of these two possible approaches would provide USF recipients an administratively feasible avenue to comply with the rule's supply chain requirements.

III. THE LIST OF PROHIBITED PRODUCTS OR MANUFACTURERS SHOULD BE DEVELOPED THROUGH A BROADER INTERAGENCY EFFORT LED BY THE EXECUTIVE BRANCH

While the FCC has targeted authority to address supply chain security issues pertaining to networks supported by USF money, the implications of the FCC's action here are potentially precedent-setting and far-reaching. Moreover, the identification of national security threats is fundamentally a function of the intelligence, law enforcement, defense and homeland security agencies of the Executive Branch, rather than that of any independent regulatory agency. Therefore, as the FCC implements this rule, it should draw on thoroughly coordinated efforts throughout the federal government in order to ensure that the supply chain security requirements or prohibitions for USF recipients are fully aligned with national security policy decisions by the Administration and/or Congress. The FCC should ensure that any further requirements or

[8] Such a list, if adopted, need not be codified in a Commission rule. The list could be generated and updated by a Bureau of the Commission, for example, or another U.S. government agency, or an independent organization identified by the Commission as authoritative on this issue.

prohibitions derive directly from broader interagency policy processes or statutory requirements that draw on expertise from throughout the government and from the private sector entities that know this complex market best.

IV. CONCLUSION

EchoStar supports Commission action to prevent universal service from being used to purchase communications equipment manufactured by companies that pose threats to the security of communications networks. The Commission should ensure that the rule is administrable, particularly by avoiding a requirement that universal service recipients determine whether equipment includes components manufactured by barred manufacturers. The FCC has a targeted role to play on these issues, but neither the FCC nor any other regulatory agency should make its own independent determinations of suspect equipment, services, and suppliers. Instead, the FCC's actions and determinations regarding USF support or other such prohibitions should derive from broader processes.

Respectfully submitted,

ECHOSTAR SATELLITE OPERATING
CORPORATION AND HUGHES
NETWORK SYSTEMS, LLC

By: _/s/____________________

Jennifer A. Manner
Senior Vice President
Regulatory Affairs

Paul Kay
Chief Information Security Officer

11717 Exploration Lane
Germantown, MD 20876

June 1, 2018