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 HUAWEI TECHNOLOGIES CO., LTD AND HUAWEI TECHNOLOGIES USA, INC.

Glen D. Nager
Bruce A. Olcott
Ryan J. Watson
Vivek Suri

JONES DAY
51 Louisiana Ave, NW
Washington, D.C. 20001
(202) 879-3939
(202) 626-1700 (Fax)

Andrew D. Lipman
Russell M. Blau
David B. Salmons
Catherine Kuersten

MORGAN, LEWIS & BOCKIUS LLP
1111 Pennsylvania Ave, NW
Washington, DC 20004
(202) 739-3000
(202) 739-3001 (Fax)

Counsel to Huawei Technologies Co., Ltd. and Huawei Technologies USA, Inc.

Date: June 1, 2018

SUMMARY

Huawei Technologies Co., Ltd. and Huawei Technologies USA, Inc. ("Huawei") applaud the Commission's objectives of protecting the nation's communications networks and supply chain, but the mechanism by which the Commission aims to do so—*i.e.*, blacklisting a handful of suppliers—is both improper and imprudent for multiple reasons. This proposal exceeds the statutory authority granted to the Commission; is arbitrary and capricious; will cause costs far in excess of any slight benefits; violates constitutional and statutory procedural requirements; and relies on unverified and unsupportable factual allegations. The Commission should not adopt its proposed rule.

First, the Commission lacks authority to prohibit USF recipients from buying equipment on the basis that a seller allegedly poses a risk to national security. To the contrary, the proposed rule would circumvent the statutory principles governing the USF, which seek to ensure that reasonably priced, high quality telecommunications and broadband services are available in rural, insular, and high cost areas. The Communications Act directs the Commission to base its USF program on specific, enumerated principles—none of which reference national security concerns. The omission reflects Congressional intent to withhold this authority from the Commission, as it has in the same Act explicitly empowered the President, as Commander in Chief, to make policies in furtherance of national security. Courts have long declined to interpret a statute as conferring authority on an agency that Congress did not intend to grant. The Commission's cited sources of authority for its NPRM are unpersuasive and fail in the face of statutory language expressly defining the scope of the agency's universal service authority.

Second, the proposed rule is both vague and irrational, and contravenes the reasoned decisionmaking scheme prescribed by the Administrative Procedure Act. The NPRM does not define

"national security" or establish any criteria for deciding which companies to blacklist. If a company is accused of being a "threat" to national security, the proposed rule offers neither a procedural vehicle nor a substantive standard by which it could challenge that accusation. Furthermore, the proposed rule draws impermissible and irrational lines by targeting specific sellers, rather than equipment, apparently on the basis of their national origin. In doing so, the Commission ignores the realities of global telecommunications supply chains. The proposed rule would prohibit the use of USF funds to purchase equipment from companies such as Huawei because its headquarters are in China, but would permit purchases from other companies with a substantial footprint in China, including multiple offices, manufacturing facilities, supply chain vendors, and even a joint venture with the Chinese Government. This is clear evidence that the proposed rule is arbitrary. The solution is not to blacklist even more companies, but to identify and address actual threats to the supply chain without drawing such arbitrary and irrational lines.

Third, the purported benefits of the proposed rule are speculative and outweighed by the substantial costs it would pose, indicating that the Commission lacks a rational basis to issue the rule. To begin with, the Commission has no method to identify or evaluate the validity of an alleged threat to national security. The NPRM fails to assess the complexities of global supply chains, which make the wholesale blacklisting of companies based on their country of origin an ineffectual means of guarding against purported bad actors. The NPRM also does not take into consideration the degree of cybersecurity risk for USF recipients, many of whom are small, rural entities, school districts, or libraries, and not only represent a small fraction of U.S. telecommunications networks, but are also unlikely targets of cyberattacks. Conversely, the proposed rule would cause significant harm to the U.S. telecommunications market by decreasing competition and increasing costs to

both USF recipients and American consumers. This, in turn, would impede the deployment of important emerging telecommunications technologies, such as 5G.

Fourth, the proposed rule deprives companies of notice and a meaningful hearing before placing them on a blacklist that, by virtue of its very existence, causes injury to corporate reputation. This would contravene the Due Process Clause, the Communications Act, and the Administrative Procedure Act, all of which guarantee a company the opportunity to review and respond to evidence against it. Moreover, under the Due Process Clause, the Commission—as well as any other agency the Commission may consider delegating the task to—is legally prohibited from using rulemaking to brand a list of companies as "national security threats" and bar sale of their equipment to USF recipients. In fact, the Commission demonstrates no lawful, reasoned method for determining whether a company is a national security threat, instead impermissibly proposing to use existing statutes enacted for entirely different purposes, such as the 2018 National Defense Authorization Act, or even other agency decisions to debar a company.

Last, the Commission lacks the factual basis to designate Huawei as a "threat" as it clearly intends to do under proposed rule. The Commission does not analyze Huawei's longstanding commitment to the security of telecommunications networks nor its continued, active participation in improving global cybersecurity standards. Instead, it prejudges Huawei wholly on the location of its headquarters. The Commission provides no evidence that Huawei equipment poses, or has posed, a national security threat and instead relies entirely on unspecified and unverified allegations, primarily a 2012 report from the House Permanent Select Committee on Intelligence that misinterprets an outdated Chinese law no longer in existence. Furthermore, not only does Chinese law *not* provide the Chinese government with the authority to interfere in private companies, but it also offers substantial protection for corporate enterprises *from* the government. Huawei has not

engaged in harmful conduct, and the Commission can point to no rational, factual reasons to believe that it may do so at some theoretical point in the future.

Huawei is committed to ensuring the security and integrity of communications networks and the telecommunications supply chain. However, while Huawei fully supports the Commission's intent behind the NPRM, it cannot support a rulemaking that is irrational, arbitrary, divorced from the facts, and contrary to U.S. laws and the Constitution. As such, Huawei urges the Commission to decline to adopt the proposed rule and terminate this rulemaking proceeding.

Table of Contents

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

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

COMMENTS OF HUAWEI TECHNOLOGIES CO., LTD
AND
HUAWEI TECHNOLOGIES USA, INC.

Huawei Technologies Co., Ltd. and Huawei Technologies USA, Inc. (collectively, "Huawei"), by its undersigned counsel, submits these comments in response to the Notice of Proposed Rulemaking ("NPRM") released in this docket (FCC 18-42) on April 18, 2018, by the Federal Communications Commission ("FCC" or "Commission") and published in the Federal Register on May 2, 2018 (83 Fed. Reg. 19196).

I. INTRODUCTION

Huawei appreciates the Commission's commendable interest in protecting the security and integrity of the communications networks and the communications supply chain, objectives profoundly shared by Huawei. However, Huawei considers the manner by which the Commission proposes to further that goal to be fundamentally flawed. As an initial matter, the Commission lacks authority to promulgate the rule proposed in the NPRM because it exceeds the Commission's statutory authority. Furthermore, even if such action were within the Commission's purview, the rule would still be impermissible because it is arbitrary and capricious in several respects under the Administrative Procedure Act ("APA"). And, in addition to these flaws, the rule violates the due process rights of targeted companies by blacklisting them and thereby depriving them of rights

without an opportunity for an individualized hearing. Huawei believes the Commission should abandon this misguided proposal.

The short shrift given to crucial issues in the NPRM can only lead to the conclusion that the Commission has failed to engage in the level of thorough investigation and rational analysis required by the Communications Act, the APA, and the United States ("U.S.") Constitution. The Commission has not identified any specific threat to national security nor has it made any effort to consider means of mitigating specific threats. Indeed, the Commission fails even to acknowledge the basic reality that the supply chain for telecommunications equipment is global and that the identity of the company selling such equipment says nothing about where and how the equipment's components and software were made and what national-security risks, if any, it might present. The Commission does not even claim to have done such an analysis, but instead apparently intends to rely on other parts of the Government—dealing with situations vastly different from the one here—for such analyses.

Where, as here, an agency attempts to tackle a problem beyond its authority, far outside its expertise, and in such a cursory fashion, its underlying objective must be questioned. It is difficult to avoid the conclusion that the Commission has initiated this rulemaking in response to political pressure from members of Congress (among others) for the purpose of driving a small number of targeted, foreign-owned companies out of the U.S. telecommunications equipment market. Indeed, while positing that other parts of the Government (rather than the Commission itself) should designate companies that pose "threats," the NPRM specifically identifies Huawei and two other companies that the agency evidently considers candidates to be designated as suppliers from which recipients of Universal Service Fund ("USF") support could not purchase equipment or services.

The NPRM does not identify proper statutory authority for such an approach. Nor does it treat like situations alike—contrary to the APA. And it does not propose to allow targeted companies any opportunity to rebut the (so-far unspecified) basis by which they would be designated a risk to U.S. national security. As Huawei has been the target of sustained political attacks by various U.S. Government officials for several years based on the locations of its headquarters—and not upon any specific incident or other factual evidence—Huawei can only conclude that the Commission has initiated this rulemaking for no other purpose than to target Huawei (and the other named companies) in response to such political pressure and on the same factually unfounded basis, without any evidence of any actual threat to national security or any reason to believe that blacklisting would result in any meaningful increase in network or supply chain security.

As Professor Emily Hammond notes in her expert report on conventions of adjudication, "[m]any of our country's darkest moments are marked by exercises of legislative power against individuals without due process of law." Exhibit H, Declaration and Expert Report of Emily Hammond ("Hammond Decl.") 18. The FCC's procedurally defective proposal—namely, "[u]sing a rulemaking proceeding to blacklist entities" in the context of a federal program—"harkens back" to these dark moments, such as the notorious "era of McCarthyism," and "is anathema to the rule of law and the U.S. Constitution." *Id.*

In sum, the proposed rule is irrational, arbitrary, divorced from the facts, contrary to the law, and at odds with the U.S. Constitution. The Commission should abandon this misguided approach and, instead, allow industry standards-based efforts to progress in order to more effectively protect the security and integrity of communications network and supply chains—particularly for entities that receive U.S. support and their customers or users—and, ultimately, U.S. national security.

II. HUAWEI'S INTEREST IN THE PROPOSED RULE

A. Huawei Technologies Co., Ltd.: Business Overview

Huawei Technologies Co. Ltd is a global leader in information and communications technology ("ICT") products and services. Huawei Technologies Co., Ltd. was established in 1987 exclusively through private investment in Shenzhen, Guangdong Province—a special economic zone where market-oriented reforms were first introduced in China—where it is still headquartered. Although the company initially focused on providing connectivity to unserved rural areas of China, it expanded first domestically, and ultimately began serving international customers at the end of the following decade. Huawei launched Research & Development ("R&D") centers in India, Sweden, and the U.S. by 2001, the same year it began business operations in the U.S. Huawei has always been, and remains today, a private company wholly owned by its founder and its employees through an Employee Stock Ownership Plan, in which 80,818 employees participated at the end of 2017. Exhibit C, Declaration of Thomas Dowding ("Dowding Decl.") ¶¶ 10-11.

Huawei's products and services encompass four sectors. *Id.* at ¶ 8. First, Huawei supports international carriers through its Internet of Things ("IoT"), All-Cloud, and 5G offerings, among other telecommunications products and services. *Id.* Second, Huawei's enterprise business supports nearly 200 Fortune Global 500 companies through its products in cloud, big data, OpenStack software tools, data centers, and IoT. *Id.* Third, as a top three international phone maker by sales, Huawei's growing consumer business offers world-class smart devices—in 2017 alone, for example, Huawei shipped 153 million smartphones worldwide. Fourth, Huawei's Cloud Business Unit was launched in 2017 and includes a service portfolio of 99 services across 14 major categories, with applications in manufacturing, healthcare, e-commerce, and connected vehicles. *Id.*

Huawei's multinational operations support more than 500 major telecommunications operators across more than 170 countries. *Id.* at ¶ 7. Currently, 45 of the world's 50 largest telecommunications providers are Huawei customers. Huawei's significant global footprint is further evidenced by the fact that about 60% of Huawei revenue is generated outside Mainland China. To provide sustainable equipment and service to its customers, Huawei established a global supply chain and procure components, spares, equipment, software, service from suppliers located in U.S., Europe, Asia and other regions. Thus, Huawei equipment consists of elements supplied by a number of established, reputable companies, such as Qualcomm, Broadcom, IBM, Microsoft, Intel, Amazon, Oracle, SAP, Cummins, ADI, Amphenol, Kingston, Siemens, Schneider, ABB, Salesforce, Red Hat, NXP, Kohler, MTU, STMicroelectronics, TSMC, Toshiba, Infineon, MTK, and Grundfos. Huawei's procurement from U.S. suppliers account for a large portion of its supply chain—in the last 4 years, Huawei has procured more $20 billion from over 1,600 U.S. suppliers.

Huawei is committed to innovative design and technological progress. Nearly 40% of its employees are engaged in R&D across 16 research centers, 26 joint innovation centers, and 45 training centers, spanning countries including the U.S., Canada, the United Kingdom ("U.K."), Pakistan, France, Germany, Colombia, India, Israel, Russia, and Turkey. In 2017, Huawei invested $13.8 billion on R&D—more than Google parent's Alphabet, ranking Huawei sixth in the world,[1] and representing a 17.4% increase compared with Huawei's 2016 expenditure. *Id.* at ¶ 12. Of this, hundreds of millions went to innovative R&D initiatives in the U.S.

[1] IRI - The 2017 EU Industrial R&D Investment Scoreboard, http://iri.jrc.ec.europa.eu/scoreboard17.html#modal-one.

Huawei's corporate governance structure spans a number of different groups and committees. At the highest level, corporate oversight of Huawei is carried out by a Board of Directors (the "Board"), which is responsible for, among other things, reviewing and approving all plans for entering industries or strategic changes; organizational restructuring; financial policies and business transactions; internal controls and operational compliance systems; and the employment of senior management. The Board and its Executive Committee are led by rotating chairmen. Currently, the Board comprises 17 private citizens. *Id.* at ¶ 16. Huawei also employs an independent auditor. Since 2000, Huawei's auditor has been KMPG.[2]

As Huawei has become increasingly global, it has attracted top talent internationally to support its business and operations. For example, Huawei's global head of cybersecurity is John Suffolk, formerly employed by the U.K. government as Her Majesty's Government Chief Information Officer. Huawei is also actively involved in supporting and contributing to the formulation of international standards, with membership in more than 300 standards organizations, including prolific standards organizations such as IEEE-SA, ETSI, OpenStack, and CCSA.

B. Huawei Global Cybersecurity Policies

As both an important social responsibility and a key commercial interest, Huawei considers cybersecurity paramount—so much so that it has affirmed at the highest levels that its commitment to cybersecurity will not be superseded by other commercial interests. Huawei has established an end-to-end global cybersecurity system through stringent security policies and processes in every facet of its global operations that reflect international standards and guidelines, local laws and

---

[2] Huawei: Independent Auditor, *available at* http://www.huawei.com/en/about-huawei/corporate-governance/independent-auditor.

regulations, and feedback from vendors, employees, suppliers, and customers. Dedicated committees and offices within Huawei implement and oversee enterprise-wide governance of cybersecurity and privacy policies and procedures. In short, cybersecurity is simply part of the company's DNA. Exhibit B, Declaration of Donald Purdy, Jr. ("Purdy Decl.") ¶¶ 10-18.

For example, Huawei's supply chain security management system is designed to be traceable, transparent, and secure. They are derived from ISO 27000 standards and include ISO 27001 certification. *See* Exhibit I, Huawei Cyber Security White Paper (June 2016) 20-21.[3] Huawei's supplier management system is ISO 28000-compliant and includes a rigorous audit checklist that selects suppliers based on their contribution to the quality and security of Huawei products and services. *Id.* Huawei also uses an IT system to monitor and visualize the logistics of supplier transport, thereby ensuring the authenticity and integrity of its parts and products. *Id.* at 22-24.

Similarly, Huawei has implemented other procedures to ensure the security of customer information and networks, such as using a secure solution to ensure that customer data is not transferred to Huawei corporate networks without customer permission. Purdy Decl. ¶¶ 25, 33. In addition, Huawei strictly manages all employees with access to customer networks through policies based on ISO 27001 and other standards for employee network management—including letters of commitment that detail roles, responsibilities and potential legal liabilities—and requiring further training and testing on cybersecurity issues. *Id.* at ¶¶ 29-32; Dowding Decl. ¶ 17.

[3] http://www.huawei.com/en/about-huawei/cyber-security/whitepaper/huawei-cyber-security-white-paper-2016.

Huawei's commitment to cybersecurity spans across all employees and through its corporate leadership by implementing a robust internal compliance program that includes routine processes for self-checks. Purdy Decl. ¶¶ 17, 22-23. All key internal business groups and functions are required to follow detailed cybersecurity policies and processes. *Id.* at ¶ 13. Business units are subject to annual performance requirements that include cybersecurity and privacy protection criteria. *Id.* at ¶ 15. Cybersecurity and privacy compliance is similarly an important metric for reviewing individual managers and employees. *Id.* Huawei's employees are incentivized to fully correct any problems that are identified, as nonconformance with the company's detailed cybersecurity policies directly impacts merit pay, annual increases, retention and promotions. *Id.* Furthermore, Huawei ensures that all its products are subject to rigorous testing for known vulnerabilities, malicious code, and hidden functionality. *Id.* at ¶ 24; *see also* Exhibit O, Certification and Testing of Huawei Products. Such testing is undertaken by internal, expert labs operating independently of the business units that are responsible for designing and producing the products.

Huawei has dedicated significant resources to continually refining its cybersecurity policies to ensure that they reflect the latest innovation and changes in industry standards. Huawei actively contributes to numerous standards-setting organizations and governmentally driven discussions on cybersecurity best practice, which not only allow Huawei to stay informed of new cybersecurity developments, but also provide an opportunity to share the results of Huawei's continued research into protecting the integrity and security of networked solutions. In this vein, Huawei also publishes substantial white papers on cybersecurity, which are available to the public. *See* Huawei Cyber Security White Paper (June 2016); Exhibit J, Huawei Cyber Security White

Paper (Dec. 2014);[4] Exhibit K, Huawei Cyber Security White Paper (Oct. 2013);[5] Exhibit L, Huawei Cyber Security White Paper (Sept. 2012).[6]

Huawei also has filed comments with this Commission in a number of proceedings relating to cybersecurity and network security generally, as well as other technical issues, and has cooperated closely with Commission staff in these areas. *See, e.g.,* Reply Comments of Huawei Technologies, Inc. (USA) and Huawei Technologies Co., Ltd., *In the Matter of Expanding Consumers' Video Navigation Choices and Commercial Availability of Navigation Devices,* Docket Nos. 16-42, 97-80 (filed May 16, 2016); Comments of Huawei Technologies, Inc. (USA), *In the Matter of the FCC's Public Safety and Homeland Security Bureau Requests Comments on CSRIC IV Cybersecurity Risk Management and Assurance Recommendations,* Docket No 15-68 (filed May 29, 2015). In addition, Huawei draws upon the support and expertise of globally respected professional firms such as IBM for processes and technology, Accenture for customer relationship management, the Hay Group for HR processes, PricewaterhouseCoopers for finance, and KPMG for auditing. These consultancies and others have helped to reinforce Huawei's management and organizations structure, forming the foundation upon which Huawei's business has prospered.

C. Huawei U.S. Operations

Huawei launched operations in the United States in 2001 through Huawei Technologies USA, Inc. ("Huawei Technologies USA"); Huawei Device USA Inc.; and Futurewei Technologies, Inc. ("Futurewei") (collectively, "Huawei-USA"), all Texas corporations headquartered in

---

4 http://www.huawei.com/en/about-huawei/cyber-security/whitepaper/hw_401493.

5 http://www.huawei.com/en/about-huawei/cyber-security/whitepaper/hw_310548.

6 http://www.huawei.com/en/about-huawei/cyber-security/whitepaper/white-paper-2012.

Plano, Texas, and governed by U.S. laws. Dowding Decl. ¶¶ 18-19. Huawei Technologies USA is comprised of the carrier, enterprise, and solar business groups. Huawei Device USA focuses on Huawei's consumer business. Futurewei focuses on R&D in the U.S.

Huawei-USA brought advanced technology and much needed competition to the U.S. For example, Huawei's 4T4R Single Radio Area Network ("RAN") products helped its U.S. carrier clients improve their service area coverage by 30%. *Id.* at ¶ 29. Huawei-USA is able to offer competitive prices due to the relatively high costs of wireless infrastructure in the U.S., a market dominated by two European companies.

Although the trajectory in Huawei-USA's sales was on the rise through its first decade serving the U.S. market, sales have declined since roughly 2012. This coincided with the conclusion of the investigation, and release of the final report, of the House Permanent Select Committee on Intelligence ("HPSCI") which, despite the lack of evidence of an actual risk to U.S. national security, encouraged private sector entities to use vendors other than Huawei. *See* Permanent Select Committee on Intelligence, U.S. House of Representatives, Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE (Oct. 8, 2012) ("2012 HPSCI Report")That report and ongoing agitation and interference by various U.S. Government officials and agencies in private business dealings between Huawei and both existing and prospective customers have continued to stymie Huawei-USA's business growth. *See, e.g., id.* at ¶ 33.

In spite of these challenges, Huawei has never faltered in its commitment to the U.S. market, or to its U.S. suppliers and customers. Approximately 25% of Huawei's 263 suppliers in 2017

were U.S.-based.[7] Currently, Huawei-USA employs over 1,200 employees across 13 offices and six R&D centers in the U.S., including in Silicon Valley; Bridgewater, New Jersey; Chicago, Illinois; and San Diego, California.[8] Huawei Technologies USA currently employs approximately 280 employees, and provides ICT solutions and services to 85 active U.S. wireline and wireless carriers.

D. Huawei Technologies USA Cybersecurity Policies

Like its parent Huawei, and as its sales arm for U.S. carrier and corporate customers, Huawei Technologies USA has undertaken significant effort to ensure that its customer networks remain secure. In addition to adherence with Huawei's stringent global policies on cybersecurity and privacy, Huawei Technologies USA implements U.S.-specific policies to ensure compliance with U.S. statutes, regulations, customer requirements, and industry standards that build upon Huawei global practices. Purdy Decl. ¶¶ 19-20. Huawei Technologies USA has a separate Cybersecurity and Privacy Committee chaired by its Chief Security Officer, with members appointed by Huawei Technologies USA executives. *Id.* at ¶ 21. Huawei Technologies USA conducts internal, semi-annual checks of cybersecurity and privacy. *Id.* at ¶ 22.

Huawei Technologies USA designs, develops, and deploys its products and software subject to strict cybersecurity protocols. Huawei-USA's business is strictly limited to product sales and product-related services, and does not possess access to the substantive content of any end user data. Dowding Decl. ¶ 22; Purdy Decl. ¶ 32. Where customer data is accessed with customer

---

[7] *See, e.g.*, http://www.scmp.com/business/companies/article/2143569/huawei-better-shape-withstand-us-pressure-thanks-industrys.

[8] Huawei: Who We Are, *available at* http://usahuawei.com/who-we-are/facts-and-figures/.

consent for the purpose of servicing the equipment, Huawei Technologies USA uses a secure solution to safeguard customer data, which is isolated from the Huawei internal corporate network. *Id.* Huawei Technologies USA products and software have also been subject to third-party testing as required by carriers, including the validation of updates and patches prior to deployment. Purdy Decl. ¶¶ 33-41. In sum, Huawei Technologies USA incorporates a variety of internal and external cybersecurity processes into the lifecycle of its products and software in order to ensure that its products and software are robust against any possible malicious acts by third parties.

Just as Huawei is heavily invested in cybersecurity industry standards on an international level, Huawei Technologies USA is also an active contributor to the development of cybersecurity standards and best practices in the U.S. For example, Huawei Technologies USA consistently participates in the continued refinement of the U.S. Cybersecurity Framework by the National Institute of Standards and Technology ("NIST").[9]

III. THE FCC LACKS STATUTORY AUTHORITY TO RESTRICT THE USE OF USF FUNDS ON THE BASIS OF NATIONAL-SECURITY CONCERNS

No agency has the power to take action "in excess of statutory jurisdiction, authority, or limitations." 5 U.S.C. § 706(2)(C). Yet, as the late Justice Scalia observed, the Commission has "repeatedly been rebuked in its attempts to expand the statute beyond its text." *Talk Am., Inc.* v. *Michigan Bell Tel. Co.*, 564 U.S. 50, 69 (2011) (Scalia, J., concurring); *see, e.g.*, *ACA Int'l* v. *FCC*,

[9] *See, e.g*, Comments of Huawei Technologies, Inc. (USA) and Huawei Technologies, Co., Ltd., *Information on Current and Future States of Cybersecurity in the Digital Economy*, National Institute of Standards and Technology, Docket No. 160725650-6650-01 (filed Sept. 9, 2016); "Developing a Framework to Improve Critical Infrastructure Cybersecurity," Submission from Huawei Technologies to the National Institute of Standards and Technology, Docket No. 130208119–3119–01 (filed Jun. 1, 2017).

885 F.3d 687 (D.C. Cir. 2018); *All Am. Tel. Co.* v. *FCC*, 867 F.3d 81 (D.C. Cir. 2017); *Montgomery County* v. *FCC*, 863 F.3d 485 (6th Cir. 2017); *Bais Yaakov of Spring Valley* v. *FCC*, 852 F.3d 1078 (D.C. Cir. 2017). The proposed rule is yet another legally unauthorized action: The Commission has no statutory authority to prohibit USF recipients from using USF funds to buy equipment sold by companies supposedly subject to foreign influence and thereby allegedly presenting a threat to national security.

A. The Commission Lacks Authority to Adopt Universal-Service Policies in the Supposed Name of Promoting National Security

Agencies must make rules on the basis of the factors that Congress directs them to consider, not on the basis of other factors of their own choosing. For one thing, agencies have an obligation to comply with statutory commands—including commands about what the agency may consider and what it may not. For another thing, "an agency rule would be arbitrary and capricious if the agency has relied on factors which Congress has not intended it to consider." *Motor Vehicle Manufacturers Ass'n v. State Farm Mutual Auto Ins. Co.*, 463 U.S. 29, 43 (1983).

No one doubts that the promotion of national security is a legitimate goal for a government to pursue. Congress, however, has not assigned the role of pursuing that goal to the Commission—at least not in this context. Specifically, the Communications Act does not give the Commission authority to adopt universal-service policies in the supposed name of "promot[ing] … national security." NPRM, ¶ 36. On the contrary, the text of the statutory provisions addressing universal service, as well as the Communications Act as a whole and general principles of administrative law and statutory interpretation, legally bar the proposed rule. In brief:

- Section 254 directs the Commission to make USF decisions only on the basis of principles that are enumerated in § 254(b) or are prescribed through a specific statutory mechanism, and such principles do *not* include national-security concerns.

- Congress has expressly empowered the President to consider national-security concerns in certain other parts of the statute, but conspicuously failed to empower the Commission to do so in the context of the USF program.

- If Congress wanted to grant the Commission the politically, diplomatically, and constitutionally significant power to make USF decisions on the basis of national-security concerns, it would surely have said so explicitly.

1. Text of Section 254.

Section 254, the provision of the Communications Act that addresses universal service, provides that the Commission "shall base policies for the preservation and advancement of universal service" on a textually enumerated set of "universal service principles." 47 U.S.C. § 254(b). These enumerated universal-service principles include making "quality services … available at just, reasonable, and affordable rates," promoting "access to advanced telecommunications and information services … in all regions of the Nation," ensuring that rates in "rural, insular, and high cost-areas" remain "comparable to rates charged for similar services in urban areas," and promoting "access to advanced telecommunications services" for schools, "health care providers, and libraries." *Id.* Importantly, these enumerated universal-service principles do not include the promotion of foreign-policy or national-security objectives (such as minimizing foreign influence on telecommunications in the U.S.). Much less do these principles authorize the Commission to promote such objectives at the expense of the enumerated principles. Indeed, two features of the statute establish that the Commission may not rest universal-service policies on such foreign-policy or national-security objectives.

First, the statute states that the Commission "shall base" USF actions on the statutorily specified universal-service principles. "The enumeration presupposes something not enumerated." *Gibbons* v. *Ogden*, 9 Wheat. 1, 195 (1824) (Marshall, C.J.). And, "the expression of one thing implies the exclusion of others." *Jennings* v. *Rodriguez*, 138 S. Ct. 830, 844 (2018). In other words,

the use of statutorily stated principles is mandatory, not discretionary, and the enumeration of a carefully defined set of universal-service principles implies that the Commission may not pursue other, unrelated goals through USF actions—much less take actions that impede the statutorily specified policies.

Second, the statute prescribes a mechanism for establishing new universal-service principles beyond those set forth in the statutory text: "The [Federal-State Joint Board on Universal Service (the "Joint Board")] and the Commission" may adopt "such other principles as [they] determine are necessary and appropriate for the protection of the public interest, convenience, and necessity and are consistent with this chapter." § 254(b)(7). Under this procedure, the Joint Board first recommends the establishment of an additional universal-service principle, and the Commission then decides whether to ratify the proposal. *See, e.g.*, *Federal-State Joint Board on Universal Service*, 12 FCC Rcd 87, ¶ 23 (1996) (Joint Board's recommendation to establish an additional principle of "competitive neutrality"); *In the Matter of Fed-State Joint Board*, 12 FCC Rcd 8776, ¶¶ 46–47 (1997) (Commission's adoption of this recommendation); *Federal-State Joint Board on Universal Service, Lifeline and Link-Up*, 25 FCC Rcd 15598, ¶ 75 (2011) (Joint Board recommendation of additional principle of support for "advanced services"); *Connect America Fund*, 26 FCC Rcd 17663, ¶ 45 (2011) (Commission's adoption of this recommendation).

There would have been no point to requiring that the Joint Board and the Commission jointly adopt new universal-service principles through this procedure if the Commission could, as it seeks to do here, just unilaterally consider whatever factors it wished anyway. Indeed, "it would be unreasonable under this statutory scheme to infer that [the Commission] retains inherent authority to short-circuit or end-run the carefully prescribed statutory process." *Ivy Sports Medicine, LLC* v. *Burwell*, 767 F.3d 81, 87 (D.C. Cir. 2014).

Unsurprisingly, therefore, the Tenth Circuit has held that "the FCC may exercise its discretion to balance the principles against one another when they conflict, but may not depart from them altogether to achieve some other goal." *Qwest Corp.* v. *FCC*, 258 F.3d 1191, 1200 (10th Cir. 2001). Likewise, the D.C. Circuit has held that "the Commission may not depart from the principles in § 254(b) altogether to achieve some other goal." *Rural Cellular Ass'n* v. *FCC*, 588 F.3d 1095, 1102 (D.C. Cir. 2009).

The proposed restriction on the use of universal-service funds—*i.e.*, prohibiting the purchase of equipment from companies supposedly subject to foreign influence—violates these features of the statutory scheme. The proposed restriction does not serve any of the goals established in § 254(b): It does not make quality services "available at just, reasonable, and affordable rates," promote "access to advanced telecommunications and information services … in all regions of the Nation," or the like. Although the NPRM includes boilerplate language reciting a few of these principles in one paragraph, it never explains how the proposed rule would advance those principles. NPRM, ¶ 35. The proposed restriction instead serves an entirely different goal: minimizing supposed "foreign state influence" on the American telecommunications market. *Id.* at ¶ 5. Neither Congress nor the Joint Board (with the Commission's approval) has ever established that goal as a universal-service principle. The proposed restriction thus does no more and no less than "depart from the principles of § 254(b) altogether to achieve some other goal." *Qwest*, 258 F.3d at 1200. It is therefore unlawful.

In fact, the Commission's proposed restriction is doubly unlawful, because it *thwarts* the achievement of the statutorily enumerated universal-service principles. For example, the universal-service principles direct the Commission to ensure that "consumers in all regions, including … those in rural, insular, and high cost areas, … have access to telecommunications and information

services … that are reasonably comparable to those services provided in urban areas," all "at rates that are reasonably comparable to rates charged … in urban areas." § 254(b)(3). Yet far from *expanding* the availability of telecommunications in rural, insular, and high-cost areas, the proposed rule may *restrict* it—by preventing the use of USF funds for equipment purchases that would promote such expanded services. *See* Section V.B below (explaining that the proposed rule could have significant detrimental effects on universal-service objectives, including disproportionately harming small rural U.S. carriers). It is self-evident that restricting recipients' choice of vendors can only create obstacles to the achievement of the statute's goals. This frustration of the statutory objectives underscores the unlawfulness of the proposed rule.

2. Context.

It is a "fundamental canon of statutory construction that the words of a statute must be read in their context and with a view to their place in the statutory scheme." *Utility Air Regulatory Group* v. *EPA*, 134 S. Ct. 2427, 2441 (2014). One specific application of this general principle is that, "where Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion." *Russello* v. *United States*, 464 U.S. 16, 23 (1983). As a result of this interpretive presumption, courts usually "refus[e] to find implicit in ambiguous sections of [a statute] an authorization to consider [a factor] that has elsewhere, and … often, been expressly granted." *Whitman* v. *Am. Trucking Ass'n*, 531 U.S. 457, 468 (2001).

Yet, elsewhere and often, the Communications Act expressly grants—while also limiting—legal authority to adopt policies under which foreign-policy or national-security concerns are dispositive. These provisions grant the power to make certain policies on the basis of national-security concerns to the President (who has specified constitutional responsibilities for national

security), not to the Commission. *See* Section III.A.3 below (discussing this point in detail). For example: Section 305(c) empowers "the President" to authorize foreign governments to operate radio stations near their embassies in Washington, D.C., if "he determines it to be consistent with and in the interest of national security." Section 308 empowers the Commission to suspend ordinary licensing procedures "during a national emergency proclaimed by the President." Section 606(a) empowers "the President," during "a war," to direct carriers to give priority to "such communications as in his judgment may be essential to the national defense and security." Section 606(c) empowers "the President" to order "the closing of any station for radio communication" during "a war," "if he deems it necessary in the interest of national security or defense." Section 606(d) empowers "the President" to "suspend … the rules … applicable to … facilities or stations for wire communications," if the President determines that "there exists a state or threat of war" and that the suspension is "in the interest of the national security and defense."

More broadly, as Professor Hammond's expert report details, numerous other statutes expressly grant agencies the power to make determinations on the basis of national security. Hammond Decl. 9-14. When Congress grants such authority, it typically includes "special structural and procedural protections"—for instance, hearing requirements, reporting requirements, and the involvement of agencies with national-security expertise—to guard against "arbitrariness and unfounded exercises of power." *Id.* at 10. Congress has taken this approach in statutes granting authority relating to national security to (among others) the Department of Commerce, the Federal Energy Regulatory Commission, the Nuclear Regulatory Commission, the Office of Management and Budget, the General Services Administration, and the Federal Aviation Administration. *Id.* at 11–14 (collecting examples).

The universal-service provisions, in stark contrast, include no comparable authorization to act on the basis of foreign-policy or national-security concerns (much less authorizations to treat these concerns as dispositive). Nor do these provisions explicitly set out procedures that the agency must follow when making decisions on the basis of such concerns. Courts would thus "presum[e] that Congress acted intentionally and purposely" in this "disparate inclusion [and] exclusion." *Russello*, 464 U.S. at 23. And they would "refus[e] to find implicit" in the universal-service provision an authorization to consider national security that has "elsewhere, and so often, been expressly granted." *Whitman*, 531 U.S. at 468. The Commission's contrary approach is not legally proper.

3. Principles of Administrative Law.

Three principles of administrative law and statutory interpretation reinforce this reading of § 254 and the Communications Act as a whole.

First, courts will not interpret a statute to confer authority on an agency to act where it is "unlikely that Congress would leave" the issue in question for determination by that agency. *MCI Telecomm. Corp.* v. *AT&T Co.*, 512 U.S. 218, 231 (1994). For example, in *Dep't of Navy* v. *Egan*, 484 U.S. 518, 531 (1988), the Supreme Court held that the civil service laws did not give the Merit Systems Protection Board the power to review revocations of security clearances, because the Court "consider[ed] it extremely unlikely that Congress intended" to "involve the Board" in making "national security determinations." Similarly, in *King* v. *Burwell*, 135 S. Ct. 2480, 2489 (2015), the Court held that the Affordable Care Act did not grant the Internal Revenue Service the power to determine the availability of certain tax credits, because it was "especially unlikely that Congress would have delegated this decision to the IRS, which has no expertise in crafting health insurance policy." So too, in *Epic Sys.* v. *Lewis*, 2018 WL 2292444, at *11 (2018), the Court held that the National Labor Relations Act did not grant the National Labor Relations Board the power

to regulate workplace arbitration agreements, because "dispute resolution procedures" were far removed from "union organization and collective bargaining"—"the bread and butter of the NLRA." It is likewise "extremely unlikely" that Congress would have granted *the FCC* the power to make universal-service policies under which national-security concerns are dispositive. Such concerns are beyond the Commission's institutional responsibility and expertise.

The Constitution vests the power to make decisions about "national security affairs" in "those who are best positioned and most politically accountable for making them"—Congress and the President. *Hamdi* v. *Rumsfeld*, 542 U.S. 507, 531 (2004) (plurality opinion). The Constitution vests in Congress important national-security responsibilities, such as the declaration of war, the raising of armies, the regulation of the military, and all power to make law addressing national-security concerns. *See* U.S. Const. art. I, § 8. The Constitution, in addition, makes the President the Commander in Chief and "the Nation's organ in foreign affairs." *Am. Ins. Ass'n*v. *Garamendi*, 539 U.S. 396, 414 (2003). Specifically, the President, where legally authorized, is the Nation's voice, and has "the prerogative" for "national security policy," *Ziglar* v. *Abbasi*, 137 S. Ct. 1843, 1862 (2017)—subject, of course, to other constraints such as the Due Process Clause, which apply fully to presidential actions taken in the realm of national security. The Commission, by contrast, has no constitutionally conferred authority over either foreign affairs or national security and can only act as constitutionally authorized by Congress.

In addition, foreign policy and national security lie outside the Commission's area of "expertise." *King*, 135 S. Ct. at 2489. The Commission has "substantial expertise" on "telecommunications" policy. *U.S. Telecom Ass'n*v. *FCC*, 825 F.3d 674, 710 (D.C. Cir. 2016). But the Commission "has neither aptitude, facilities nor responsibility" to make "delicate [and] complex"

judgments concerning national security and foreign affairs. *Chicago & Southern Air Lines* v. *Waterman S.S. Corp.*, 333 U.S. 103, 111 (1948). It is thus "extremely unlikely that Congress intended" to "involve the [Commission]" in making national-security policy. *Egan*, 484 U.S. at 531.

Indeed, the Commission is an independent regulatory agency; its commissioners are not subject to the will and direction of the President, and thus "cannot in any proper sense be characterized as an arm or eye of the executive." *Humphrey's Ex'r* v. *United States*, 295 U.S. 602, 629 (1935). Although case law allows Congress to create such independent agencies for administering certain domestic policies in constitutionally appropriate circumstances, *id.*, courts have also recognized that Congress may not do so where it would "impede the President's ability to perform his constitutional duty," *Morrison* v. *Olson*, 487 U.S. 654, 691 (1988). Further, it has never been suggested that Congress could authorize an independent agency to conduct the Nation's foreign affairs or national-security policy—areas where the President has express constitutional responsibilities and even more expansive legislatively conferred authorities. *See Hamdi*, 542 U.S. at 531; *Webster* v. *Doe*, 486 U.S. 592, 606 (1988) (O'Connor, J., concurring in part and dissenting in part); *Garamendi*, 539 U.S. at 414. Principles of constitutional avoidance thus counsel against interpreting the Communications Act to give the Commission authority to label a company a "national security threat" and bar purchases of its equipment with USF funds. *Edward J. DeBartolo Corp.* v. *Florida Gulf Coast Bldg. & Constr. Trades Council*, 485 U.S. 566, 574 (1988).

In the end, however, there is no need to address any such profound constitutional question, much less to speculate about what Congress is likely to have intended, because the Communications Act itself displays Congress' unwillingness to lodge in the Commission the power to make such national-security judgments on USF matters. Every single time the Communications Act expressly grants the power to make a judgment on the basis of national security, it defines the specific

power and vests that power in the President—not in the Commission. Section 305(c) empowers "*the President*" to authorize foreign governments to operate radio stations near their embassies if "*he determines* it to be consistent with and in the interest of national security." Section 606(a) empowers "*the President*," during "a war," to direct carriers to give priority to "such communications as in *his judgment* may be essential to the national defense and security." Section 606(c) empowers "*the President*" to order "the closing of any station for radio communication" during "a war," "if *he deems* it necessary in the interest of national security or defense." Section 606(d) empowers "*the President*" to "suspend … the rules … applicable to … facilities or stations for wire communications," if the President determines that "there exists a state or threat of war" and that the suspension is "in the interest of the national security and defense." At no point did Congress grant such authority with regard to the USF program to either the President or the Commission, and it must thus be presumed to have foreclosed additional measures in this particular field. *See Youngstown Sheet & Tube Co.* v. *Sawyer*, 343 U.S. 579, 639 (1952) (Jackson, J., concurring).

Second, and quite apart from the foregoing principles, courts presume that Congress "does not … hide elephants in mouseholes." *Whitman*, 531 U.S. at 468. In other words, Congress does not use "modest words" to grant an agency a "highly significant" power. *Id.* For example, in *MCI*, 512 U.S. at 231, the Supreme Court held that the Communications Act did not implicitly grant the Commission the power to exempt carriers from tariff filing requirements, because it was "highly unlikely" that Congress would delegate an issue of such "enormous importance" through "subtle" implications. And in *FDA* v. *Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 147 (2000), the Court held that the Food, Drug, and Cosmetic Act did not implicitly grant the Food and Drug Administration the power to regulate tobacco, because, "given the economic and political significance of the tobacco industry …, it is extremely unlikely that Congress could have intended to

place tobacco within the ambit of the [agency] absent any discussion of the matter." The same is true here for the Commission's claim to power to restrict use of USF funds on the basis of national-security concerns.

The power to make national-security policy has vast "political significance." *Brown & Williamson*, 529 U.S. at 147. As one commenter has already noted, foreign governments may take umbrage at an insinuation that they are hostile to the U.S., that they will refuse to honor the independence of their corporations, or that they intend to tamper with American telecommunications networks. *See Ex parte* submission by David S. Addington, NFIB, WC Docket No. 18-89, at 3-4 (filed April 5, 2018). Moreover, prohibiting purchase of equipment from companies on the ground that they are supposedly "subject to foreign influence" can hugely, and adversely, affect the reputations and viability of those enterprises.

Congress cannot be presumed to have silently left to an independent agency such as the Commission the power to make USF decisions that would be fraught with such serious diplomatic, political, and economic consequences. These kinds of foreign-policy and national-security decisions historically and conventionally are within the domains of Congress and, then, the President. An intent instead to give authority over such decisions to an administrative agency—particularly an independent agency—could be found only in an express statutory text. No such text grants the Commission such authority to consider national-security concerns in the context of USF funding decisions; in fact, as noted above, the statutory text and the statute as a whole show the contrary intent.

Third, "when an agency claims to discover in a long-extant statute an unheralded power to regulate" a new subject, courts "typically greet its announcement with a measure of skepticism."

Utility Air, 134 S. Ct. at 2444. Put another way, "when an agenc[y] assert[s] power" in "new arenas," courts tend to "perform a close and searching analysis" of its decision, "remaining skeptical of the proposition that Congress did not speak to such a fundamental issue." *ACLU* v. *FCC*, 823 F.2d 1254, 1567 n.32 (D.C. Cir. 1987).

Under these principles, the lack of precedent for the Commission's assertion of authority to regulate universal service in the name of national-security concerns undermines the Commission's claim of statutory authority to do so. The Communications Act has empowered the Commission to address universal service since its enactment in 1934; indeed, the preamble to the original Communications Act states that one of the statute's purposes was "to make available, so far as possible, to all the people of the United States a rapid, efficient, Nation-wide, and world-wide wire and radio communication service." 47 U.S.C. § 151 (1934). Yet only now, 84 years later, has the Commission asserted, for the first time, that it may rest universal-service policies on its judgments about national security—and that, in doing so, it may even impede the provision of communications services to all of the people. The sheer novelty of the assertion lays bare its incredibility and unsoundness.

In the final analysis, all of these points boil down to the "fundamental" rule that an agency "may not bootstrap itself into an area in which it has no jurisdiction." *Adams Fruit Co.* v. *Barrett*, 494 U.S. 638, 650 (1990). Or, as the Supreme Court more recently put it, an agency "threatens to undo rather than honor legislative intentions" when it adopts an "expansive interpretation" of its own authority in order to seize the power to regulate a matter in which it has no "expertise." *Epic Systems*, 2018 WL 229244, at *14. That is exactly what the Commission is doing here. The Commission's delegated authority encompasses the making of rules to promote "quality services … at just, reasonable, and affordable rates," "access to advanced telecommunications and information

services … in all regions," and so forth. § 254(b). The Commission may not use that authority to "bootstrap itself" into an area—national security—"in which it has no jurisdiction" or "expertise," and, in doing so, may *undermine* the provision of universal services.

B. The Commission's Contrary Arguments Are Unpersuasive

The NPRM cites a series of statutory provisions as the sources of the Commission's asserted authority to prohibit USF recipients from buying equipment sold by companies supposedly posing a risk to national security. None of the cited provisions is up to the task of supporting the proposed restriction, and none can overcome the statutory limitations just discussed.

1. Sections 201(b) and 254(c)(1)(D).

Section 201(b) grants the Commission general authority to "prescribe such rules and regulations as may be necessary in the public interest to carry out the provisions of this chapter." Section 254(c)(1)(D) states that "universal service is an evolving level of telecommunications services that the Commission shall establish periodically under this section," and provides that, when the Commission "establish[es] the definition of the services that are supported by Federal universal service support," it must "consider the extent to which such telecommunications services … are consistent with the public interest, convenience, and necessity." The NPRM asserts that, in the USF context, "the promotion of national security is consistent with the public interest." NPRM, ¶ 36. That assertion is inconsistent with any reasonable interpretation of the statute.

The Supreme Court has "consistently held" that "the words 'public interest' in a regulatory statute" grant an agency only a bounded authority to promote "the purposes of the regulatory legislation," not "a broad license to promote the general public welfare." *NAACP* v. *FPC*, 425 U.S. 662, 670 (1976). In other words, the power to make rules in the "public interest" is the power to promote the goals of the specific regulatory program at hand—not the power to promote other,

unrelated objectives (no matter how important or admirable those other objectives might be). For example, the Interstate Commerce Commission's power to regulate in the "public interest" is the power to ensure "adequacy of transportation service"—not the power to stamp out "unfair labor practices" among railroads. *Id.* And the Federal Power Commission's power to regulate in the "public interest" is the power to "promote the orderly production of plentiful supplies of electric energy and natural gas"—not the power "to eradicate … employment discrimination" among energy companies. *Id.* at 670–71; *see Massachusetts v. EPA*, 549 U.S. 497, 533 (2007) (similarly concluding that the statutory term "'judgment' is not a roving license [for the Environmental Protection Agency] to ignore the statutory text," but is merely "a direction to exercise discretion *within defined statutory limits*") (emphasis added).

These interpretive principles also apply to the Communications Act. The Supreme Court has specifically held that the phrase "public interest" in the Communications Act "is to be interpreted by its context," and "is not to be interpreted as setting up a standard so indefinite as to confer an unlimited power." *Nat'l Broadcasting Co.* v. *United States*, 319 U.S. 190, 216 (1943). For instance, where the Commission regulates radio, "the 'public interest' to be served … is … the interest of the listening public in the larger and more effective use of radio." *Id.* at 216. Similarly, where the Commission regulates broadcast licenses, the "public interest" is the interest in ensuring that programming "fairly reflects the tastes" of the audience." *NOW* v. *FCC*, 555 F.2d 1002, 1017 (D.C. Cir. 1977). In that context, the "public interest" does not include the interest in avoiding "sex discrimination"—so that the Commission may not withhold a broadcast license solely on the ground that a broadcaster has violated the civil-rights laws. *Id.*

In the context of universal service, the "public interest" is the interest in promoting the purposes of the statute's universal-service provisions. There is no need to guess what those purposes are; § 254(b) expressly enumerates them and states that the Commission "shall" base its policies on them. Sections 201(b) and 254(c)(1)(D) thus take the Commission back to the universal-service principles already discussed. They do not empower the Commission to invoke other unrelated factors such as national-security concerns.

The NPRM cites a decision of the Tenth Circuit for the proposition that "nothing in [§ 254(c)(1)] limits the FCC's authority to place conditions … on the USF funds." NPRM, ¶ 35 (quoting *In re FCC 11-161*, 753 F.3d 1015, 1046 (10th Cir. 2014)). In fact, that judicial decision expressly reaffirms the rule that "the FCC may exercise its discretion to balance the [universal-service] principles against one another when they conflict, but may not depart from them altogether to achieve some other goal." 753 F.3d at 1055. The court there emphasized that it was upholding the funding conditions imposed in that case only because they were "consistent … with § 254(b)'s express charge to the FCC to 'base policies for the preservation and advancement of universal services' on a specific set of controlling principles outlined by Congress." *Id.* at 1047. The Tenth Circuit in no way countenanced funding directives that go beyond those principles. *Id.* But that is what the proposed rule unlawfully seeks to do here.

2. Section 254(b)(7).

The NPRM next cites § 254(b)(7), which empowers the Commission and the Joint Board to adopt "such other" universal-service principles as they actually "determine are necessary and appropriate for the protection of the public interest, convenience, and necessity and are consistent with this chapter." When Congress authorized the Commission to administer the USF in the Telecommunications Act of 1996, as noted in section III.A above, it enumerated specific principles to

govern the USF. Significantly, the language of Section 254(b) is mandatory—the Commission "shall" base its universal service policies on these principles. The Notice suggests that this provision empowers the Commission to ensure "that USF funds are used to deploy infrastructure and provide services that do not undermine our national security." NPRM, ¶ 36. This suggestion is doubly flawed.

As an initial matter, the Commission's invocation of § 254(b)(7) is procedurally defective. That provision empowers "the Joint Board *and* the Commission" jointly to adopt certain new universal-service principles. The Joint Board has not recommended a new universal-service principle to cover national-security concerns, much less has the Commission accepted any such recommendation. Unless and until the Joint Board and Commission properly adopt a new principle through the statutorily specified procedure, the Commission may not rest its invocation of a new universal-service principle on § 254(b)(7).

In any event, even if the Joint Board were to concur, the Commission lacks the authority to make "the promotion of national security" (NPRM, ¶ 36) a universal-service principle. Section 254(b)(7) provides for the adoption of "other" universal principles that are in "the public interest" and "consistent with this chapter." "Promotion of national security" does not qualify as an "other principle" within the meaning of § 254(b)(7). The interpretive rule known as *ejusdem generis* "limits general terms that follow specific ones to matters similar to those specified." *Christopher* v. *SmithKline Beecham Corp.*, 567 U.S. 142, 163 n.19 (2012). The catchall reference to "other principles" thus covers only "other principles" that are similar to the universal-service principles already expressly specified. It is not properly read to include "the promotion of national security," a subject both far removed from "affordable rates" and access "in rural, insular, and high cost areas," and beyond the expertise and historical province of the Commission.

Similarly, the phrase "public interest" is not properly read to cover the "promotion of national security." As just discussed, the phrase "public interest" in a regulatory statute refers to the interest in promoting the goals of the regulatory program at hand; it is not a general license to promote the public good. For the reasons noted above, the purposes of the universal-service program do not encompass "the promotion of national security," and, indeed, are incompatible with the restriction being proposed. *See* Section III.A above.

Further, treating the "promotion of national security" as a new universal-service principle would not be "consistent with this chapter." In the rest of "this chapter"—that is, in the rest of the Communications Act—Congress took pains to specify the circumstances under which it authorized telecommunications policy to consider national-security concerns (and by whom). Congress repeatedly and explicitly defined the situations in which national-security concerns could be dispositive under the statute, and conferred the power to make the pertinent judgments on the President, not on the Commission. *See* Section III.A.3 above. For the Commission to use § 254(b)(7) to vest in itself the power to make national-security judgments in the context of USF matters is inconsistent with that statutory scheme, and, since the Commission is independent of the politically accountable actors constitutionally charged with such responsibilities, constitutionally problematic.

3. Section 254(e).

The NPRM also invokes § 254(e), which provides that universal-service funding recipients "shall use that support only for the provision, maintenance, and upgrading of facilities and services *for which the support is intended*." (Emphasis added.) The Notice suggests the Commission has the authority to determine that universal-service funds are not "intended" to support services that undermine national security. NPRM, ¶ 36. This, too, is legally erroneous.

Just like the general public-interest standard, § 254(e) merely takes the Commission back to the same universal-service principles already discussed above. It does not empower the Commission to rest a prohibition on the use of funds on additional factors, such as concerns about foreign influence, that go beyond those principles.

Indeed, the Commission has previously interpreted the phrase "for which the support is intended" to refer to the congressional "intent" reflected in the "principles set forth in section 254(b)." *Connect America Fund*, 26 FCC Rcd at ¶ 64. Because agencies have an obligation to follow their own regulations, the Commission must follow that interpretation here. *See United States ex rel. Accardi* v. *Shaughnessy*, 347 U.S. 260, 266 (1954).

4. Section 151.

The NPRM also cites the preamble to the Communications Act, which "describes the development of a 'Nation-wide … wire and radio communication service, for the purpose of the national defense' as one of the reasons for establishing the Commission." NPRM, ¶ 36 (quoting 47 U.S.C. § 151). That preambular reference to national defense also does not authorize the proposed regulation.

"It frustrates rather than effectuates legislative intent simplistically to assume that *whatever* furthers the statute's primary objective must be the law." *Rodriguez* v. *United States*, 480 U.S. 522, 526 (1987) (emphasis original); *see also Encino Motorcars, LLC* v. *Navarro*, 138 S. Ct. 1134, 1142 (2018) (reiterating this principle). Here, it frustrates rather than effectuates legislative intent simplistically to assume that, just because the preamble refers to "national defense," the statute can be read to give the Commission authority to do anything that could be thought to promote the national defense. That is particularly true when the body of the Communications Act shows that

Congress explicitly entrusted *the President*, not the Commission, with making the (discrete) defense-related judgments for which the Communications Act calls.

In all events, "the body of the statute" takes precedence over a "preamble" that is "inconsistent" with it. *Price* v. *Forrest*, 173 U.S. 410, 427 (1899). And "it is a commonplace of statutory construction that the specific governs the general." *Morales* v. *Trans World Airlines, Inc.*, 504 U.S. 374, 384 (1992). Section 254(b)'s universal-service principles appear in the body of the Communications Act and deal specifically with universal service. The general reference to "national defense," by contrast, appears in the preamble and deals generally with the Communications Act as a whole. To the extent these provisions conflict, the more specific textual provisions of § 254(b) take precedence over the more general prefatory provisions of § 151. And under the provisions of § 254(b), the Commission has no authority to use universal-service funding as a vehicle for making national-security policy, much less to undermine statutory universal-service principles while seeking to further national-security policies of the Commission's own making.

5. Section 1004.

The NPRM further proposes to "rely" on 47 U.S.C. § 1004, which provides: "A telecommunications carrier shall ensure that any interception of communications or access to call-identifying information effected within its switching premises can be activated only in accordance with a court order or other lawful authorization and with the affirmative intervention of an individual officer or employee of the carrier." The Notice appears to suggest that prohibiting funding recipients from buying equipment sold by companies who are supposedly subject to foreign influence is a way to enforce this statutory obligation. That argument is incorrect.

The link between § 1004 and the proposed prohibition is (to put it mildly) exceedingly remote. Section 1004 imposes an obligation on *all* telecommunications carriers; the proposed rule,

by contrast, imposes restrictions only on recipients of universal-service funding. In addition, § 1004 addresses one highly specific risk (the risk of interceptions "effected within [the] switching premises"); the proposed rule, by contrast, addresses an entirely separate risk ("foreign state influence," NPRM, ¶ 5). The Commission identifies no reason to believe that "foreign state influence" on the *seller* of equipment will manifest itself through an "interception … effected within [the] switching premises" of the *carrier*. At the very least, any connection between foreign-state influence on equipment sellers and interceptions within switching premises is too attenuated to support the adoption of the proposed rule. *Cf.* Antonin Scalia & Bryan A. Garner, *Reading Law* § 30 (2012) ("Predicate-Act Canon") ("Despite the story describing how 'for want of a nail the kingdom was lost,' the authority to protect the kingdom does not reasonably imply the authority to promulgate standards for the shoeing of horses").

6. Section 256 policy goals

The NPRM does not cite, much less consider, the policy goal identified by Congress in § 256, which directs the Commission "to promote nondiscriminatory accessibility by *the broadest number of* users and *vendors of communications products and services* to public telecommunications networks used to provide telecommunications service …." 47 USC § 256(a) (emphasis supplied). The rule proposed in the NPRM would have the exact ***opposite*** effect by arbitrarily limiting the number of vendors who can offer products and services for use on these networks.

This is not a case where the Commission has found that the burden of reducing the accessibility of the broadest number of vendors to public telecommunications networks is offset by some other benefit the statute authorizes the Commission to pursue. Rather, the Commission has not even acknowledged the issue, or sought comments on the magnitude of the burden. *See Michigan v. EPA*, 135 S. Ct. 2699, 2707 (2015) (quoting *Motor Vehicle Manufacturers Ass'n*v. *State Farm*

Mutual Auto. Ins. Co., 463 U.S. 29, 43 (1983)) (holding that "an agency may not entirely fai[l] to consider an important aspect of the problem when deciding whether regulation is appropriate.") (internal citations omitted). Hence it cannot possibly conduct the required rational examination of the issue based on the NPRM.

7. Consideration of national security in other settings

The NPRM also asserts that the Commission "considers national security, law enforcement, and foreign policy concerns in the course of" making certain other decisions—implying that the Commission may therefore consider similar concerns when making universal-service policy. NPRM, ¶ 8. Even assuming without conceding the legality of the Commission's approach in these other contexts, the Commission's conclusion simply does not follow from the premise.

As an initial matter, one key distinction sets the universal-service provisions apart from all of the other provisions that the Commission cites: The universal-service provisions, unlike all of the other provisions, include an exhaustive list of statutorily specified principles to guide the Commission's decisions—and those principles make no reference to national security. Thus, irrespective of whether the Commission may properly consider certain national-security concerns in some other situations, Congress has not authorized it to consider such concerns in the USF context.

In any event, the analogies cited by the Commission are unconvincing on their own terms. The first provision that the Commission cites, § 214, grants the Commission power to license the construction and extension of new telecommunications lines when "public convenience and necessity require." But § 214(b) entitles "the Secretary of Defense" and (in some cases) "the Secretary of State" to "notice" and "the right … to be heard" in such licensing proceedings—arguably implying that defense and foreign-policy concerns *are* relevant to such proceedings. Even then, the provision implicitly recognizes that it is not *the Commission's* role to determine in the first

instance whether a license is consistent with the needs of national defense and foreign policy; that is precisely why the Communications Act gives the Secretaries of Defense and State the opportunity to appear and to set out those interests. The universal-service provisions, in stark contrast, grant no such right of participation to the Secretary of Defense or the Secretary of State. They thus do *not* even arguably presuppose the relevance of national-security concerns.

Similarly, another provision that the Commission cites, § 310(b), allows the Commission to refuse a broadcasting license to an entity that is controlled by a corporation with more than "one-fourth" foreign ownership, "if the Commission finds that the public interest will be served by the refusal." Again, one might rationally argue that national security and foreign policy are relevant in the context of a provision that deals specifically with foreign-owned corporations. The universal-service provisions, by contrast, include no such contextual clue suggesting the potential relevance of national security and foreign policy in this distinct context.

Last, the Commission cites the Submarine Cable Landing Act. That Act is distinct from the Communications Act and thus has little relevance to the interpretation of the latter statute. Moreover, the Submarine Cable Landing Act vests "the *President*" with the power to license the landing and operation of submarine cables connecting the United States with foreign countries. 47 U.S.C. § 34 (emphasis added). The Commission exercises authority with respect to such cables only because the President has delegated the authority to it by executive order. Executive Order 10530 § 4, 19 Fed. Reg. 2709 (1954). The functions that the President entrusted to the Commission under the Submarine Cable Landing Act say nothing about the functions that Congress entrusted to the Commission under the Communications Act's universal-service policies.

8. "National Security."

The NPRM, last of all, invokes the general importance of "national security" as a justification for the agency's actions. No one contests the vital importance of protecting the national security of the U.S. Yet "there are limitations … in the powers authorized by congressional enactments, even with respect to matters of national security." *Ziglar*, 137 S. Ct. at 1861. "And national-security concerns must not become a talisman used to ward off inconvenient claims—a 'label' used to 'cover a multitude of sins.'" *Id.* at 1862. Indeed, the "danger" of unlawful action is "heightened," not lessened, when an agency invokes national-security concerns, "given the difficulty of defining the security interest" in question. *Id.* Put simply, the Commission may not use the label "national security" to gain an authority that is lacking in the statutory scheme and yet that is necessary to support the proposed USF rule. Nor may the Commission rely on broad notions of "public interest" untethered to specific statutory authorization. *See Massachusetts*, 549 U.S. at 533 ("while the President has broad authority in foreign affairs, that authority does not extend to the refusal to execute domestic laws").

IV. THE PROPOSED RULE IS ARBITRARY AND CAPRICIOUS

Agency action is unlawful if it is "arbitrary [and] capricious." 5 U.S.C. § 706(2)(a). This means that, even when an agency pursues a "legitimate" goal, it still "must do so in some rational way." *Judulang* v. *Holder*, 565 U.S. 42, 55 (2011). The lines drawn by the agency must reflect "non-arbitrary, relevant factors." *Id.* "Normally, an agency rule would be arbitrary and capricious if the agency has relied on factors which Congress has not intended it to consider, entirely failed to consider an important aspect of the problem, offered an explanation for its decision that runs counter to the evidence before the agency, or is so implausible that it could not be ascribed to a difference in view or the product of agency expertise." *State Farm*, 463 U.S. at 43.

A. The Proposed Rule Fails to Meet the Requirements of Notice-and-Comment Rulemaking and Is Arbitrary and Capricious Because It Is Unduly Vague and Offers No Meaningful Guidance to Affected Parties

The proposed rule consists of only a single paragraph that makes a vague reference to "national security." It does not define "national security," and it does not give any hint how that term will be defined and applied. This proposal is so vague that it forces interested parties to "divine the agency's unspoken thoughts," depriving them of a meaningful "opportunity to develop evidence in the record to support their objections to the rule." *Envtl. Integrity Project v. EPA*, 425 F.3d 992, 996 (D.C. Cir. 2005). Indeed, the proposed rule's unelaborated reference to "national security threats" is, in addition, arbitrary and capricious, because it "fails to articulate a comprehensible standard … and offers no meaningful guidance to affected parties." *ACA Int'l*, 885 F.3d at 700. Moreover, even if the Commission's proposed rule constitutes a "comprehensible standard," it is arbitrary and capricious for the additional reasons discussed below.

B. The Proposed Rule is Arbitrary and Capricious Because it Draws Irrational Lines

The proposed rule is also arbitrary and capricious because it draws irrational lines. It is a "fundamental norm of administrative procedure" that "an agency [must] treat like cases alike," and "dissimilar treatment" of similar cases is "the quintessence of arbitrariness and caprice." *Westar Energy, Inc.* v. *FERC*, 473 F.3d 1239, 1241 (D.C. Cir. 2007). For this reason, "'an agency's unjustifiably disparate treatment of two similarly situated parties works a violation of the arbitrary-and-capricious standard.'" *LePage's 2000, Inc.* v. *Postal Reg. Comm'n*, 674 F.3d 862, 866 (D.C. Cir. 2012) (*per curiam*) (internal citation omitted); *see also Anna Jaques Hosp.* v. *Sebelius*, 583 F.3d 1, 7 (D.C. Cir. 2009) ("'Where an agency applies different standards to similarly situated entities and fails to support this disparate treatment with a reasoned explanation and substantial

evidence in the record, its action is arbitrary and capricious and cannot be upheld.'") (internal citation omitted). Courts repeatedly have relied on this principle when invalidating or directing agencies' actions. *See Melody Music, Inc.* v. *FCC*, 345 F.2d 730, 732 (D.C. Cir. 1965) (holding that an agency's "refusal at least to explain its differential treatment" of two similarly situated companies was error); *see also Capital Cities Commc'ns, Inc.* v. *FCC*, 554 F.2d 1135, 1139 (D.C. Cir. 1976) (remanding for, among other things, "a reconsideration of the problem of unequal treatment of petitioners and others similarly situated"); *NLRB v. Gen. Stencils, Inc.*, 438 F.2d 894, 904 (2d Cir. 1971) (vacating and remanding because, among other reasons, the agency had not fulfilled its "duty to explain its imposition of a remedy in one case and its failure to do so in a seemingly similar—or even stronger—one"); *Bracco Diagnostics, Inc.* v. *Shalala*, 963 F. Supp. 20, 24, 27–28 (D.D.C. 1997) (granting preliminary injunctive relief because the agency had likely "treat[ed] similarly situated people differently").

These principles apply with even greater force where an agency pursues an objective that differs from the ones on which Congress directed the agency to focus. Where an agency chooses to "consider factors that are not mentioned explicitly in the governing statute," it must "spell out in more detail" than usual "how [its] decision … can be squared with the statutory objectives that Congress specified as the primary guidelines for administrative action in this area." *Indep. U.S. Tanker Owners Comm.* v. *Dole*, 809 F.2d 847, 854 (D.C. Cir. 1987).

Here, the proposed rule itself is, as noted, completely lacking in definition or detail. Moreover, it claims only to pursue the objective of promoting "the security of America's communications networks." NPRM, ¶ 1. But Congress nowhere directed the Commission to consider this factor in making USF policies. To the extent that the agency can consider this factor at all, it must at least "spell out in more detail" than usual its justifications for its actions. The Commission,

however, has done no such thing. It never explains how the proposed rule pursues its stated objective in a rational way. Instead, the Commission arbitrarily singles out certain companies for blacklisting, without any evidence that equipment sold by those companies poses any greater threat to national security than equipment sold by other companies.

1. The proposed rule irrationally targets particular sellers rather than equipment

The proposed rule's arbitrariness begins with the proposal to target particular *sellers* rather than particular *equipment*. The Commission expressly proposes to restrict the use of USF funds to buy, not equipment that poses a national security threat, but "equipment produced or provided by any company posing a national security threat." Proposed Rule, 47 C.F.R. § 54.9. That approach is unsupportable.

Any rule that turns on the identity of the seller rather than the nature of the equipment would be dramatically over-inclusive. A seller that fits the Commission's test for allegedly posing a "national security threat" may nonetheless make or sell a wide range of products that are entirely safe. For instance, the company might sell products that have been tested and certified as secure. Or it might sell simple products that are inherently incapable of posing any kind of risk to national security—fiber optic cables, antennas, and amplifiers, to name a few examples. There is no justification for a blunderbuss approach that sweeps in such innocuous items.

At the same time, any rule that turns on the identity of the seller rather than the nature of the equipment would also be dangerously under-inclusive. Sellers that are not covered by the Commission's rule—and thus escape the Commission-imposed "national security threat" label—may still sell products that are vulnerable to hacking, misuse, or interference by foreign states. Yet on the Commission's proposed seller-centered approach, funding recipients would remain wholly free

to buy and use such equipment, supposedly introducing "security vulnerabilities in communications networks" across the country. NPRM, ¶ 3. This under-inclusiveness is so serious that it undermines the Commission's claim to be protecting national security—and lends credence to the possibility that the Commission is responding to political pressure, or engaging in invidious discrimination against certain foreign companies. *Cf. Williams-Yulee* v. *Florida Bar*, 135 S. Ct. 1656, 1668 (2015) ("underinclusiveness can raise doubts about whether the government is in fact pursuing the interest it invokes").

2. The proposed rule impermissibly ignores the realities of telecommunications supply chains

The proposed rule is more arbitrary still because it ignores the reality that, as the Suffolk Declaration explains, the supply chain for telecommunications equipment is global. *See generally* Exhibit A, Declaration of John Suffolk ("Suffolk Decl.") 1 ("The ICT supply chain is global"). The Commission names Huawei and ZTE as companies that could supposedly pose national-security risks because they come from, and make some of their equipment in, China. NPRM, ¶ 4. Yet at the same time, the Commission seemingly would allow the continued use of equipment made by other companies that have manufacturing facilities in China (or any other country that might pose an alleged national-security risk), embed components imported from China, use software written by Chinese programmers, or have other ties to China.

The global telecommunications supply chain is a complex and dynamic landscape in which determining risk truly requires an individualized analysis of who manufactures particular equipment, its components, and software; where that work is done; the arrangements under which that happens (*e.g.*, a joint venture with a state-owned enterprise, a wholly-owned subsidiary, *etc.*); and the ability of a foreign state or other malicious actor to introduce backdoors or other vulnerabilities

given these factors. And because this "supply chain is global, security risks arise from the cumulative supply chain, not the vendor whose name happens to be on the 'box' or who provides the named application." Suffolk Decl. 3. But the Commission proposes to do none of this necessarily complex risk assessment, instead simply drawing a line based on the country of origin of the final seller of a product or service—even though "[t]he name of the vendor, or vendor's home country, does not determine the source of the product and cannot be used as a key criterion for a source of threat." *Id.* at 2. In so doing, the Commission draws an arbitrary and discriminatory line that inevitably would both fail to address significant supply chain risks and block equipment that poses no more threat than equipment that remains allowed.

To give just one example: The Commission seemingly would allow the continued use of USF funds to buy equipment made by Nokia, while seeking to prohibit the use of such funds to buy equipment made by Huawei. But the Commission fails to explain why Huawei's equipment should be prohibited while Nokia's equipment is allowed. Nokia, too, has ties to China. Indeed, Nokia itself concedes that "essentially all major information technology and communications companies have global supply chains, many of which include sourcing of components from China and elsewhere." Nokia April 18 Comments at 1-2. Further, Nokia has "six Technology Centers," "one regional Service Delivery Hub," and "more than 80 offices" in China.[10] Moreover, in 2017, Nokia formed a joint venture with the Chinese Government, Nokia Shanghai Bell Co. *Id.*; *see also* Suffolk Decl. 2 (noting that "some of [Nokia's] equipment is made in China, with components purchased from Chinese companies, and indeed Nokia has a joint venture with a Chinese Government-

[10] Nokia Form 20-F, https://www.sec.gov/Archives/edgar/data/924613/000155837018002320/nok-20171231x20f.htm.

owned entity, Nokia Shanghai Bell"); Exhibit M, Nokia Signing a Joint Venture Agreement with China Huaxin to Establish Nokia Shanghai Bell. Unlike Huawei (a private company), that joint venture is directly supervised by the State-Owned Assets Supervision and Administration Commission of the State Council. Exhibit N, Nokia 2016 Corporate Social Responsibility Report of Shanghai Nokia Bell.[11]

It is true that Nokia has entered into national-security agreements with the U.S. Government, but the Commission never suggests that Huawei could resolve the Commission's concerns by entering into a similar agreement. If a national-security agreement is enough to cure supposed threats to national security, the Commission should indicate what terms it requires in such an agreement, so that Huawei and others can evaluate them. In the meantime, the Commission has no authority to give companies preferential treatment.

To be clear, Huawei is in no way suggesting that Nokia poses a national-security threat or that it should be precluded from selling to USF-funded buyers. Rather, the point is that, just as Nokia's ties to China do not undermine the safety of Nokia's equipment, Huawei's ties to China also do not undermine the safety of Huawei's equipment. For the Commission to fail to recognize this point—and thereby to allow Nokia, but not Huawei, to sell its equipment to USF recipients—is to violate the "fundamental norm of administrative procedure" that "an agency [must] treat like cases alike." *Westar Energy*, 473 F.3d at 1241.

---

[11] Ericsson also has "several joint venture companies in China, including production companies, since the Chinese government demands local manufacturing. One important company is Nanjing Ericsson Communication Company Ltd., which was established with the electronics manufacturer Nanjing Panda Electronics." *See* https://www.ericsson.com/en/about-us/history/places/asia/china. *See also* Suffolk Decl. 2 ("Ericsson … also has a joint venture with a Chinese Government owned entity").

3. The proposed rule utilizes arbitrary methods to identify blacklisted sellers

The methods by which the Commission proposes to identify the sellers to be blacklisted introduce an additional layer of arbitrariness.[12]

Under the Commission's proposals, a seller could be deemed a threat to national security in the context of USF if another governmental entity has deemed it a threat to national security in a more sensitive context (such as nuclear defense). For instance, relying on the National Defense Authorization Act for Fiscal Year 2018, Pub. L. 115-91, 131 Stat. 1283, 1762, Sec. 1656 ("2018 NDAA"), the Commission at one point suggests that any seller barred from supplying equipment to the programs covered by that statute would also be barred from supplying equipment to USF recipients. NPRM, ¶ 21. The 2018 NDAA, however, only bars the "Department of Defense" from using the covered companies' equipment in "certain critical programs, including ballistic missile defense and nuclear command, control, and communications." NPRM, ¶ 6. The Commission thus appears to believe that, because Congress concluded that a particular company's equipment was too risky to use in ballistic-missile and nuclear-command programs, yet safe enough to allow in other Department of Defense programs, that company's equipment is too risky to allow in *rural*

[12] Indeed, the proposals discussed in this section, if adopted, likely would violate the Due Process Clause. *See* Section VI.C. But a reviewing court could invalidate them as arbitrary and capricious for the reasons stated here, without reaching the Constitutional question.

schools and libraries (the kinds of places covered by USF funding). This leap from ballistic-missile programs to elementary schools and rural libraries reveals a loss of all sense of proportion and rationality, and underscores the arbitrariness of the Commission's proposal.[13]

Moreover, to the extent that the 2018 NDAA (or any other governmental report or decision) is premised on the false notion that Chinese laws require Chinese telecommunications companies to cooperate with China's government to engage in espionage and cyber attacks, reliance on such legislation and reports is deeply flawed. As the Declaration of Jihong Chen and Jianwei Fang explains, neither Article 13 of the Counterespionage Law, Article 18 of the Anti-Terrorism Law, nor Article 28 of the Cyber Security Law requires that a company such as Huawei, let alone an overseas subsidiary such as Huawei Technologies USA, cooperate with the Chinese government in this manner. Exhibit E, Declaration of Jihong Chen & Jianwei Fang ("Chen & Fang Decl.") ¶¶ 8-9. Nor, as a factual matter, has such cooperation occurred at Huawei or Huawei Technologies USA. *See* Purdy Decl. ¶ 42 (confirmation from the Chief Security Officer for Huawei Technologies USA that he has "never been unduly influenced by any person within Huawei, or outside of Huawei, to take any action that [he] felt was inappropriate in the assessment or management of cyber security or privacy risk"); *id.* at ¶ 45 (no knowledge of "any improper relationship between anyone associated with Huawei and anyone associated with the government of any country, including China"); *see also id.* ¶¶ 43–44.

---

[13] The Commission's reference to "pending legislation"—the Defending U.S. Government Communications Act, H.R. 4747 and S. 2391—is likewise irrational. Unless and until that legislation is enacted, of course, it has no legal force. But even if it were enacted, it would not support the Commission's proposal. For example, those bills address the use of covered technology as a substantial or essential component of a telecommunications system, while the Commission's proposed rule covers *all* uses (no matter how insubstantial or non-essential).

The Commission at another point suggests relying on past debarment decisions by other agencies—so that if another agency has excluded a company from its programs for reasons of national security, the Commission would exclude it from selling equipment to USF recipients. But this approach suffers from the same basic flaw as the last one: It fails to account for context. The fact that (for example) the Department of Defense has concluded that a particular product is insufficiently secure to use in a military base does not in any way establish that it is also insufficiently secure to use in a rural library. Further, to the extent that the other agency provided a hearing before making its debarment decision, the company would have had a reason only to present evidence and argument relevant to that other agency's decision. The company would not have known, at that time, that the hearing would also affect its eligibility to sell equipment to recipients of USF funding, and thus would have had no reason to present evidence pertinent to that distinct determination. This reality only underscores the arbitrariness with which the Commission proposes to construct its blacklist.

4. The proposed rule impermissibly equates a seller's national origin with a risk to national security

The Commission further compounds the arbitrariness of the proposed rule—and, indeed, violates the Constitution—by equating a seller's national origin with a risk to the U.S.'s national security.

The "equal protection component" of the Due Process Clause of the Fifth Amendment prohibits the Federal Government from "invidiously discriminating between individuals or groups." *Washington* v. *Davis*, 426 U.S. 229, 239 (1976). The APA likewise prohibits such action; after all, "the arbitrary and capricious standard" requires "more" than "the Due Process Clause."

State Farm, 463 U.S. at 43 n.9. An administrative agency discriminates invidiously when it imposes disabilities on account of an individual's foreign country of origin. *Hampton* v. *Mow Sun Wong*, 426 U.S. 88, 114 (1976).

The proposed rule violates these principles. At various points, the Commission appears to equate national origin (specifically, Chinese origin) with risk to U.S. security. The NPRM thus refers to "the counterintelligence and security threat posed by *Chinese* telecommunications companies" and to "suspicion [of] the continued penetration of the U.S. telecommunications market by *Chinese* telecommunications companies." NPRM ¶¶ 4, 5 (emphasis added).

But the Commission fails to explain its singular focus on "Chinese telecommunications companies"—raising an inference that it is discriminating invidiously rather than genuinely promoting national security. *See Reeves* v. *Sanderson Plumbing Prods., Inc.*, 530 U.S. 133, 147 (2000) ("Proof that the defendant's explanation is unworthy of credence is simply one form of circumstantial evidence that is probative of intentional discrimination, and it may be quite persuasive").

The NPRM myopically focuses on China (and to a lesser extent, Russia), thereby ignoring many countries that could pose national-security threats. "Pretty much every U.S. technology company manufactures its hardware in countries such as Malaysia, Indonesia, China and Taiwan," yet the Commission has never explained why the threat from companies with ties to China is any greater than the threat from (say) companies with ties to Indonesia. Bruce Schneier, *Banning Chinese phones won't fix security problems with our electronic supply chain*, Washington Post.[14] For that matter, history shows that even close allies of the U.S. could pose national-security threats.

[14] https://www.washingtonpost.com/news/posteverything/wp/2018/05/08/banning-chinese-phones-wont-fix-security-problems-with-our-electronic-supply-chain/?noredirect=on&utm_term=.9933ab752b91.

Id. Yet the proposed rule says nothing about such countries. Perhaps the Commission has an explanation for these disparities—but, if so, it has not mentioned it. This silence suggests that invidious discrimination is at work.

Moreover, a Chinese company might have similar or better cybersecurity-management processes than American or European companies. Any equipment, despite its country of origin, could be subject to national-security risks. Indeed, despite Huawei's minimal presence in the U.S., it is reported that cybersecurity attacks in the U.S. have significantly increased in recent years, suggesting that the vulnerabilities are nested in existing American networks built by other vendors.[15] These points drive home that no rational policy underlies the line that the Commission proposes to draw, further suggesting that invidious discrimination is at work here.

The procedural deficiencies of the Commission's approach heighten the inference of invidious discrimination. *See Vill. of Arlington Heights* v. *Metro. Housing Dev. Corp.*, 429 U.S. 252, 267 (1977) ("Departures from the normal procedural sequence also might afford evidence that improper purposes are playing a role."). The Commission has initiated this rulemaking with a barebones, one-paragraph proposed rule—a stark departure from the more substantial proposed rules that it typically publishes. Further, the Commission proposes to debar the "Chinese telecommunications companies" that it seeks to target without a formal hearing—even though the Due Process Clause and the Commission's own debarment regulation require such a hearing, and even though the Communications Act and APA require the hearing to provide robust procedural safeguards. *See* Sections VI.A and VI.B below. These departures from the Commission's standard

---

[15] Statista, Annual number of data breaches and exposed records in the United States from 2005 to 2017, https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.

procedures confirm that the proposed rule reflects discrimination against companies of Chinese origin.

The severity of the deprivation of liberty and the distance between the proposed rule and the Commission's responsibilities reinforce all of these points. For example, in *Mow Sun Wong*, the Supreme Court held that the Civil Service Commission discriminated invidiously by excluding aliens from certain federal jobs, even though the Commission claimed to act in order to ensure "undivided loyalty in certain sensitive positions." 426 U.S. at 104. The Court emphasized the importance "of the [private] interest at stake" and the severity of a "wholesale deprivation of employment opportunities." *Id.* at 115. It also emphasized that the agency "ha[d] no responsibility for foreign affairs." *Id.* at 114. These conclusions reflect the understanding that, where an agency that has no responsibility for foreign affairs nonetheless draws lines relating to national origin, there is an even more serious risk than usual that the classification results from xenophobia rather than from "reasons which are properly the concern of that agency." *Id.* at 116. Here, just as in *Mow Sun Wong*, the proposed rule affects a significant private interest and involves the "wholesale" denial of economic "opportunities." The discrimination would also be imposed by the FCC, an agency that does not have authority to make decisions on the basis of "foreign affairs" in the context of the USF program. *See* Section III.A above (discussing this point in detail). There is thus a serious risk that the disparate treatment of Chinese companies reflects improper bias rather than "reasons which are properly the concern of that agency."

C. The Proposed Rule is Arbitrary and Capricious Because it Reflects Irrational Decisionmaking

The proposed rule is also unlawful because it reflects irrational decisionmaking. The justifications leading up to the proposed rule are neither logical nor rational.

To start, the Commission suggests that it is appropriate to adopt the proposed rule because it has previously taken "a number of targeted steps" relating to national security. NPRM, ¶ 7. But the Commission identifies only one specific example of such a step—the adoption of rules implementing the Spectrum Act of 2012, 47 USC § 1404—and that action cannot serve as a precedent for this one, for several reasons.

First, the bar on auction participation was specifically enacted by Congress in the Spectrum Act, and the Commission's rules merely implemented that provision. Here, by contrast, the Commission proposes to act in the absence of any Congressional directive or authorization, based on an unjustified and generalized interpretation of the Commission's "public interest" mandate untethered from the actual statute itself. *See* Section III above.

Second, the Spectrum Act and the Commission's implementing rules only disqualify from bidding on contracts or in auctions "a person who has been, for reasons of national security, *barred by any agency of the Federal Government* from bidding on a contract, participating in an auction, or receiving a grant." 47 USC § 1404(c) (emphasis supplied). The statute therefore requires an act of adjudication by another agency (which presumptively would be subject to judicial review), and a specific finding that the adjudication is based on "reasons of national security," before any disqualification is imposed. The proposed rule in this proceeding contains no such safeguards.[16]

Third, the disqualification imposed by the Spectrum Act is directly related to the underlying agency decision to bar the person "from bidding on a contract, participating in an auction, or

---

[16] An "agency of the Federal Government" is generally construed as including agencies within the Executive Branch only, but not Congress or the courts. *See, e.g.,* 5 USC § 551(1). Accordingly, the Commission could not rely on the Spectrum Act to disqualify a company from obtaining a contract or bidding in an auction based solely on that company being mentioned in an Act of Congress such as the National Defense Authorization Act for Fiscal Year 2018.

receiving a grant," since the Spectrum Act simply prohibits such a person from doing the same types of things the other agency has prohibited them from doing—obtaining certain contracts and participating in auctions. Here, however, there is no apparent relationship between the predicate for designating a company as a "national security threat" and the types of transactions with USF recipients that the rule would prohibit.

Continuing its list of justifications for commencing this proceeding, the Commission acknowledges that it has created the Communications Security, Reliability and Interoperability Council ("CSRIC") to provide "recommendations to ensure the security and reliability of the nation's communications systems …." NPRM, ¶ 9. Oddly, however, the NPRM never mentions that CSRIC did deliver recommendations on cybersecurity risk management in 2015, and on supply chain security issues in 2016, which would address these concerns through design principles and processes, not by arbitrarily banning certain companies from participating in equipment markets.

By way of background, in March 2015, following 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, CSRIC IV unanimously adopted a detailed report that includes segment-specific analysis of the application of the NIST Cybersecurity Framework.[17] Then, in March 2016, Working Group 6 of CSRIC V

[17] The CSRIC IV "Cybersecurity Risk Management and Best Practices, Working Group 4: Final Report" is available at http://transition.fcc.gov/pshs/advisory/csric4/CSRIC_WG4_Report_Final_March_18_2015.pdf.

delivered a set of voluntary best practices for carriers to use when working with vendors and suppliers to reduce cybersecurity risk within the core network.[18] Although the Commission sought comment on the first of these recommendations,[19] it never took action on either one.

To be sure, the Commission is under no obligation to accept the recommendations of its expert advisors. But it is arbitrary and capricious for the Commission to fail even to consider that information and explain why it is now instead abandoning those recommendations and pursuing the proposed rule instead. Surely the CSRIC reports are relevant, as they speak directly to the very issues of supply chain security and potential cybersecurity threats that the proposed rule purports to address. The Commission's failure to explain its disregard of the CSRIC's recommendations in favor of a drastically different approach is the hallmark of arbitrary and capricious action. *See Encino Motorcars, LLC* v. *Navarro*, 136 S. Ct. 2117, 2125–26 (2016) ("Agencies are free to change their existing policies as long as they provide a reasoned explanation for the change … It follows that an unexplained inconsistency in agency policy is a reason for holding an interpretation to be an arbitrary and capricious change from agency practice."); *FCC* v. *Fox*, 556 U.S. 502, 515 (2009) ("An agency may not … depart from a prior policy *sub silentio* … And of course the agency must show that there are good reasons for the new policy").

---

[18] The CSRIC V Working Group 6 "Final Report: Best Practices Recommendations for Hardware and Software Critical to the Security of the Core Communications Network" is available at https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG6_FINAL_%20wAppendix_0316.pdf.

[19] PS Docket No. 15-68, Public Notice, FCC's Public Safety and Homeland Security Bureau Requests Comment on CSRIC IV Cybersecurity Risk Management and Assurance Recommendations, DA 15-534 (rel. Mar. 19, 2015).

In addition to the materials cited in the NPRM, Chairman Pai referred in his individual remarks to testimony before the Senate Intelligence Committee in attempting to justify the proposed rule. Of course, an individual Commissioner is not the Commission itself and, in this respect, cannot provide a rationale on behalf of the Commission. *See SEC v. Chenery Corp.*, 318 U.S. 80, 94 (1943). But apart from this, the statements the Chairman cited do not lend any meaningful support to the Commission's proposal.

The cited testimony included a statement by the FBI Director concerning "risks" of "allowing any company or entity that is beholden to foreign governments that don't share our values" to have access to key network facilities.[20] That general statement fails to address how to determine whether a foreign government does not "share our values," and, more importantly, whether a particular company is "beholden" to such a government. Moreover, Director Wray only spoke about the "capacity" of foreign companies to engage in actions hostile to the United States, not about their intent or about any actual hostile actions. Many people have the "capacity" to do harmful acts but no intention of actually doing them, so this assessment is not a sufficient basis to establish rational decisionmaking by an agency subject to the APA.

The Chairman also quoted the statement of the National Security Agency ("NSA") Director at the same hearing to the effect that the "challenge" of threats to U.S. telecommunications infrastructure will "only increase, not lessen, over time for us."[21] Because of the highly complex nature of the global supply chain and the increasing number of actors who may have authorized or unauthorized access to equipment throughout the manufacturing and delivery process, the challenge of

---

[20] Statement of Chairman Ajit Pai, FCC 18-42 at p.41 ("Pai Stmt."), n.1.

[21] *Id.*, n.3.

securing such equipment against threats is indeed likely to increase over time. Suffolk Decl. 4-5. But, as noted above, these threats come from many sources beyond those entities that sell equipment to USF recipients. If the challenge of securing the communications supply chain is increasing, it is not rational for the agency to proceed against a few target companies that could hardly be responsible for any material aspect of the issue.

Both the FBI Director and the NSA Director alluded to the possibility that classified information may exist that would shed additional light on their concerns, but of course neither Huawei nor anyone else outside the Government has any way of knowing what such information might be or show. If, however, the Government had conclusive evidence of actual misconduct by Huawei or any other Chinese technology companies operating in the U.S., it seems improbable that it would have allowed those companies to continue to operate in the U.S.. It also seems improbable that close U.S. allies that share intelligence information with the U.S. would have taken no action if they were aware of such evidence. If such evidence existed, presumably it would have been available at least at the time of the HPSCI report in 2012, yet more than five years have gone by since then and no action has been taken against Huawei, among others.

As discussed in Section VI.A.2 below, it is highly doubtful that the Commission can take any action against a company based exclusively or primarily on undisclosed classified information. But without access to or knowledge of that information, Huawei is left to guess at what the allegations against it might be. Huawei is thus put in the impossible position of trying to prove a negative.

Huawei sincerely doubts that any of its competitors could prove conclusively that none of their employees has any connection to a hostile foreign government, that none of their products has backdoors or security flaws, that their supply chain is completely secure, and that none of their

vendors and their vendors' subcontractors have any of these flaws. Indeed, there are few if any U.S. companies that could satisfactorily prove that there is no potential "risk" or "capability" of hostile action somewhere within their supply chain. It surely would be arbitrary and capricious for the Commission to hold Huawei to such an impossible standard—especially while failing to hold all companies to that same standard. *See LePage's 2000, Inc.*, 674 F.3d at 866.

D. The Proposed Rule Contradicts the Scheme of "Reasoned Decisionmaking" Established by the APA

In sum, the proposed rule contradicts the "scheme of 'reasoned decisionmaking' established by the APA." *Allentown Mack Sales & Serv., Inc.* v. *NLRB*, 522 U.S. 359, 374 (1998). "Not only must an agency's decreed result be within the scope of its lawful authority, but the process by which it reaches that result must be logical and rational." *Id.* The Commission here has been anything but logical and rational. The proposal is so vague and undefined that commenters are left to guess about what and who it covers. Further, the Commission has proposed a rule targeting particular *sellers*, even though any threat to national security would be posed by particular *equipment*. The Commission has proposed identifying the sellers by looking at what Congress and other agencies have done in the context of ballistic defense and nuclear command and control, even though the program at hand deals with schools and libraries. The Commission has focused on Chinese companies, even though companies with ties to other countries could pose similar or greater risks to national security. And, even among Chinese companies, the Commission proposes to single out a handful of companies such as Huawei, ignoring other companies whose ties to China are likewise significant. All of this, on the basis of irrational justifications and without explanation for an abrupt change in the Commission's position. "It is hard to imagine a more violent breach" of "the requirement of reasoned decisionmaking." *Id.*

V. THE PROPOSED RULE CANNOT BE JUSTIFIED BY COST–BENEFIT ANALYSIS

Without acknowledging the many costs of its proposal, the Commission requested comment on the potential costs and benefits of the proposed rule. NPRM, ¶¶ 33-34. The evidence presented below demonstrates that the costs of the proposed rule would vastly outweigh any potential benefits, and the Commission cannot rationally find otherwise. *See Michigan v. EPA*, 135 S. Ct. 2699 (2015) ("Agencies have long treated cost as a centrally relevant factor when deciding whether to regulate. Consideration of costs reflects the understanding that reasonable regulation ordinarily requires paying attention to the advantages *and* the disadvantages of agency decisions."); *Entergy Corp. v. Riverkeeper, Inc.*, 556 U.S. 208, 232 (2009) (Breyer, J., concurring in part) ("every real choice requires a decisionmaker to weigh advantages against disadvantages, and disadvantages can be seen in terms of (often quantifiable) costs").

A. The Purported Benefits of the Rule Are Speculative and Insubstantial

The premise of the proposed rule is to "ensure that universal service funds are not used in a way that undermines or poses a threat to our national security." NPRM, ¶ 2. As admirable as that goal is, the measures proposed in the NPRM would do little to achieve it.

First, the benefits of the proposed rule necessarily depend on the accuracy with which "threat[s] to our national security" are identified. But the Commission has not identified any specific threat to national security, and does not appear to have any intention of doing so. It has not even described any standards or criteria to be used in identifying such threats. Instead, it proposes to wait until another agency or branch of the Government designates one or more companies as "threats," and then use that designation to ban use of USF support to purchase products or services from that company. The Commission apparently proposes to conduct no independent inquiry into

the validity of the alleged threat, let alone any evaluation of the seriousness or accuracy of the "threat" to the Nation's telecommunications networks in particular. An assessment by another entity, in another context, and under another (unspecified) standard does not fulfill the Commission's own obligation to conduct a record-based assessment. In the absence of such an assessment, the Commission's proposed rule amounts to little more than speculation that other agencies' assessments for other purposes will happen to accurately identify companies that pose national-security threats to the Nation's telecommunications networks. That approach fails to offer any assurance that companies will not be incorrectly labeled as threats or that companies that do pose a threat will be identified. Either errors—false positives or false negatives—would render the supposed benefits of the rule illusory (or, at best, marginal).

Second, the proposed rule would address only a small portion of potential national-security threats to telecommunications networks. The proposed rule focuses on "equipment or services produced or provided by *any company* posing a national security threat …." NPRM, Appx. A, (emphasis supplied). But, as discussed above, the supply chain for telecommunications network equipment is highly complex and spans the globe. Potential vulnerabilities arise not only from the manufacturer of a finished product, but from suppliers of components and software incorporated into that product. Components produced in China are found in all forms of electronic devices from a wide range of sellers, even devices used in military applications. Exhibit G, Declaration of Bryant Tow ("Tow Decl."), ¶¶ 9-10. Moreover, third-party actors may covertly tamper with products or software before the equipment is delivered to the ultimate customer. Threats could be introduced at consolidation, border crossings, storage and distribution, or during last mile transport. *Id.* at ¶ 11. Any rule intended to address supply chain threats would have to grapple with this complexity. But the Commission simply ignores it. The proposed rule, therefore, would provide no protection

at all against a wide range of threats. The benefit of excluding a handful of targeted companies from the U.S. market would be minimal, just as locking only one of several open doors would do little to improve the security of a house.

Third, by banning all purchases from blacklisted companies, the proposed rule fails to consider whether any particular equipment or service poses "a national security threat to the integrity of communications networks or the communications supply chain." NPRM, Appx. A. The rule thus sweeps too broadly and would preclude a USF recipient from purchasing even a fiber optic cable or a battery from a company on the blacklist, even though neither purchase would pose any credible threat to national security, no matter how malicious (hypothetically) the vendor's intent might be. *See* Tow Decl. ¶ 13; Section IV.B.1 above.

Fourth, the proposed rule also fails to assess the degree of risk posed by the purchaser of the equipment or service. Many recipients of USF support are rural carriers, school districts, public libraries, and rural health care providers. Although their contributions to the development of U.S. telecommunications networks are significant (as detailed in the following section), they are not the high-value targets that a foreign government or its agents would be likely to target with cyberattacks or disruption of the supply chain. Tow Decl. ¶ 12. Because any such attack would carry a risk of retaliation, it is likely that such actions would be reserved for the highest-value targets, such as defense installations, government networks, large carriers' networks serving major metropolitan areas and the like.[22] The benefits of reducing the already-low threat of attacks targeting USF recipients, therefore, would be marginal and insignificant. Tow Decl. ¶ 20.

---

[22] Indeed, a recent analysis suggested that a hypothetical attack using hidden software code to disable a network could only work once, because the attack would immediately be detected and

B. The Costs of the Proposed Rule Would Be Massive

Because the USF supports companies throughout the Nation and in diverse segments of the telecommunications and information services markets, the costs imposed by the proposed rule would be huge—and passed through to consumers of a wide range of services. Recipients of USF support include incumbent local exchange carriers ("LECs"), wireless carriers, competitive LECs that participate in the E-Rate and Rural Health Care programs; public schools, libraries, and the vendors who provide them with E-Rate supported services, including a variety of products and services beyond traditional telecommunications services, *see* 47 CFR § 54.502(a), and health care providers and their vendors under the Healthcare Connect Fund, *see* 47 CFR § 54.634. Prohibiting targeted companies from selling their products and services to these recipients would effectively exclude these companies from significant parts of the telecommunications and information services markets in the U.S. The impact would be magnified greatly if the Commission were to adopt the interpretations discussed in the NPRM that would bar purchases from blacklisted companies by contractors and subcontractors of USF support recipients, and would prohibit such purchases in connection with any project that receives any USF funding at all. NPRM, ¶ 16. Further, the stigma created by adoption of the rule would likely discourage purchases of equipment from blacklisted companies even by customers who are not subject to the rule's terms (as may well be intended), thereby extending its effects throughout the industry and the Nation.

---

the affected equipment patched or disabled. S. Woo, "Are Huawei and ZTE a Real Threat?", *Wall Street Journal*, May 30, 2018, available at https://www.wsj.com/articles/are-huawei-and-zte-a-real-cybersecurity-threat-1527611521 (accessed May 30, 2018). It is beyond implausible that a technique that can only be used once, and could provoke "political fallout, and maybe military fallout," *id.*, would be used against (for example) a small rural cellular network.

The reduction in the number of suppliers for key categories of equipment and services will harm customers. In particular, the market for core network equipment is already highly concentrated, so eliminating even a single competitor would substantially increase prices while significantly hampering innovation. *See* Exhibit F, Declaration of Allan L. Shampine ("Shampine Decl.") ¶¶ 1-7. Currently, only three companies hold 91% of the market share for U.S. wireless infrastructure shares. *Id.* at ¶ 13. As the European Commission has noted, the mere presence of additional competitors participating in the bidding process and providing credible alternatives, regardless of whether these competitors have significant sales, benefits competition as a whole. *Id.* at ¶ 20 (citing European Commission Nokia/Alcatel Decision). Huawei's substantial international presence—holding 20-30% of the RAN market globally and 30-40% in Europe—demonstrates that its products are credible alternatives. *Id.* at ¶¶ 9-10. Notably, the Herfindahl-Hershman Index ("HHI"), which reflects market concentration such that an HHI above 2,500 is considered "Highly Concentrated" by U.S. antitrust authorities, is approximately twice as high in the United States as compared to Europe, where the HHI is reportedly below 2,300. *Id.* at ¶¶13-16,

In situations in which Huawei has been permitted to bid on requests for proposals in the U.S., its presence has reportedly resulted in increased competition and, in turn, lower prices for carriers and consumers. *Id.* at ¶ 7. Indeed, Huawei's presence in the United States has facilitated the provision of telecommunications services by dozens of small and rural providers, who are attracted by Huawei's "cheaper prices, quality products and attentive service." *Id.* at ¶¶ 23, 25. But increased competition brings benefits beyond lowered prices for Americans: it encourages and increases investment in telecommunications infrastructure as a whole. *Id.* at ¶ 24. This investment can be vital to the expedient deployment of emerging telecommunications technologies, for example 5G. *Id.* at ¶¶ 24-28. In addition, the proposed rule would upset reliance interest to the extent it

affects existing contracts. NPRM, ¶ 18. In fact, contracts have already been cancelled as a result of the NPRM, and potential customers have expressed reluctance to do business with Huawei because of the Commission's public statements casting suspicion on the company. Dowding Decl. ¶ 33.

Finally, Huawei notes that before the NPRM was adopted by the Commission, the National Federation of Independent Businesses ("NFIB") filed a letter with the Commission urging, among other things, that the Commission solicit comments on potential retaliation against American companies by foreign governments if the rule is adopted. *Ex parte* submission by David S. Addington, NFIB, WC Docket No. 18-89, at 3-4 (filed April 5, 2018). Although there are no U.S.-based manufacturers of core telecommunications network equipment, there are U.S. manufacturers of mobile handsets, operating system software, and other communications products and services that could potentially be targets of foreign retaliation. The Commission did not incorporate NFIB's suggestion into the NPRM, thereby failing to request comment on a potentially substantial additional cost that could be imposed on U.S. businesses by the proposed rule. The Commission's failure to consider this relevant factor is yet another reason why any rule adopted based on the NPRM would be arbitrary and capricious. *State Farm*, 463 U.S. at 43.

VI. THE COMMISSION MAY EXCLUDE A COMPANY FROM SELLING EQUIPMENT TO USF RECIPIENTS ONLY AFTER NOTICE AND A MEANINGFUL HEARING

The proposed rule includes no process for the companies that would be labeled "national security threats" and whose equipment USF recipients could no longer buy using USF support. But, under the Due Process Clause, the Commission may not so blacklist a company unless it first provides the company with notice and the opportunity for a meaningful individualized hearing on the charges against it. The Due Process Clause and the Communications Act both require that, at

this hearing, the Commission give the company a meaningful opportunity to review and respond to the evidence against it. Indeed, the APA requires that hearing to constitute a formal adjudication compliant with that statute's "on the record" hearing requirements.

The Commission's proposed rule complies with none of these procedural requirements. It is thus legally impermissible. Indeed, the Commission's apparent insistence on "blacklist[ing] entities" without a hearing "harkens back" to "the era of McCarthyism," and "is anathema to the rule of law and the U.S. Constitution." Hammond Decl. 18.

The Commission apparently intends to rely on shortcuts that, far from complying with the procedural requirements, merely compound the rule's constitutional and statutory defects. For example, the Commission suggests the use of rulemaking to identify a small number of companies to be blacklisted, but the Due Process Clause requires an individualized adjudication rather than a rulemaking when an agency seeks to deprive such persons of their liberty. The Commission also proposes to identify a company as a national-security risk on the basis of the 2018 NDAA, but this approach also deprives a company of its due-process right to a hearing, and it irrationally equates ballistic-missile facilities that are critical to national security (which the NDAA covers) with rural libraries (which the USF supports). Finally, the Commission proposes to define a company as a national-security risk if another agency has debarred the company for reasons of national security, but this proposal violates constitutional and legal limits on giving preclusive effect to earlier agency actions.

A. The Due Process Clause Guarantees a Company Notice and a Meaningful Individualized Hearing Before the Commission Labels It a "National Security Threat" and Restricts the Purchase of Its Equipment

The Due Process Clause of the Fifth Amendment requires the Government to provide "due process" before depriving a person of "liberty." U.S. Const. amend. V. Under this constitutional provision, the Commission may not blacklist a company until it gives the company an opportunity to be heard and to respond to the evidence against it.

1. The Due Process Clause guarantees a company notice and a meaningful hearing before it is blacklisted

"In a Constitution for a free people, there can be no doubt that the meaning of 'liberty' must be broad indeed"; the term "denotes not merely freedom from bodily restraint but also the right … to contract, to engage in any of the common occupations of life, … and generally to enjoy those privileges long recognized … as essential to the orderly pursuit of happiness by free men." *Board of Regents of State Colleges* v. *Roth*, 408 U.S. 564, 572 (1972). The term "due process" requires, "at a minimum," "notice and opportunity for hearing." *Mullane* v. *Central Hanover Bank & Trust Co.*, 339 U.S. 306, 313 (1950). Three lines of cases (some decided during the McCarthy Era, the last time federal agencies tried to blacklist people without hearings) establish that an agency deprives a company of liberty—and thus must provide the company notice and a meaningful pre-deprivation hearing—by labeling the company a "national security threat" and prohibiting the spending of federal funds on the company's products.

First, "liberty" includes the "'free liberty to sell [one's] wares in the market.'" *Sekhar* v. *United States*, 570 U.S. 729, 733 (2013) (quoting *King* v. *Burdett*, 91 Eng. Rep. 996 (K.B. 1696)). "Liberty" also includes the "freedom to practice [one's] chosen profession." *Greene* v. *McElroy*,

360 U.S. 474, 492 (1959). As a result, the government must provide notice and a meaningful hearing before taking action that "broadly precludes individuals or corporations from a chosen trade or business." *Trifax Corp.* v. *District of Columbia*, 314 F.3d 641, 644 (D.C. Cir. 2003) (addressing debarment of contractor). For example, the government must provide notice and a meaningful hearing before excluding a lawyer from the bar on account of his character. *Schware* v. *Board of Bar Exam'rs*, 353 U.S. 232, 238 (1957). So too, it must provide notice and a meaningful hearing before "foreclos[ing]" a person's "freedom to take advantage of [private] employment opportunities." *Roth*, 408 U.S. at 564.

Here, the Commission proposes to label a company a "national security threat" and deny it the right to transact freely with other private entities. Once a company is blacklisted under the proposed rule, it may no longer freely pursue its "chosen trade or business," or "sell its wares" to willing customers who wish to use USF funds to make the purchase. Under the due-process principles just discussed, that disability amounts to a deprivation of liberty. The Commission may impose such a disability, if at all, only after providing constitutionally sufficient process, including notice and a meaningful hearing on the charges made.

Second, as Professor Hammond notes in her expert report on conventions in adjudication, the Supreme Court has held that official action that imposes a "stigma" upon a person amounts to a deprivation of liberty, if that stigma is sufficiently serious to "alte[r]" the person's "status." *Paul* v. *Davis*, 424 U.S. 693, 708 (1976); *see* Hammond Decl. 7 ("a liberty interest triggering procedural due process arises where the government publicly discloses a stigmatizing statement and impacts some more tangible interest like a change of legal status"); *Siegert* v. *Gilley*, 500 U.S. 226, 234 (1991) (describing this principle as the "stigma plus" rule); *Orange* v. *District of Columbia*, 59 F.3d 1267, 1274 (D.C. Cir. 1995) ("liberty interests arise if … the government alter[s] [one's]

status in a tangible way, and … an imposition of stigma or injury to reputation accompanie[s] this change in status"). Thus, the Government must provide a person with notice and a meaningful hearing before disqualifying him from employment on grounds of alleged disloyalty. *Wieman* v. *Updegraff*, 344 U.S. 183, 191 (1952). Similarly, it must provide a person with a hearing before disqualifying him from buying liquor due to alleged alcoholism. *Wisconsin* v. *Constantineau*, 400 U.S. 433, 437 (1971).

The proposed rule would stigmatize—and injure the reputations of—any companies to which it is applied. The proposed rule declares that companies made subject to it are "national security risk[s]," are "threats" to our Nation, and are subject to "foreign state influence." NPRM, ¶¶ 1, 2, 5. As the Supreme Court explained during the years of McCarthyism, the accusation that a company threatens the security of the U.S. is a "deep" "stain" and a "badge of infamy"; it encourages the public to view the company "as a possible enemy." *Wieman*, 344 U.S. at 191. And it suggests that contracting with such a company is not only unwise, but also unpatriotic. In addition, the blacklisting of a company in this context amounts to a governmental declaration that the company is untrustworthy—that it is not dealing in good faith, but rather advancing the interests of a foreign state. *See* NPRM, ¶ 5 (quoting a statement that "'Huawei … *cannot be trusted* to be free of foreign state influence and thus poses a security threat'") (emphasis added). Such a declaration impugns the company's "good name, reputation, honor, [and] integrity." *Constantineau*, 400 U.S. at 437.

Such a stigma is sufficiently serious to alter the company's status in a tangible way. Under the proposed rule, the designation of a company as a "national security risk" has, at a minimum, the legal effect of barring the use of universal-service funds to buy the company's equipment. Moreover, the designation has the *practical* effect of discouraging other entities across the U.S.

from buying the company's equipment. How many Americans would buy products from a company that their Government has pronounced a threat to the country's national security? Indeed, the designation could have adverse effects on the company's sales and business interests across the globe. Put simply, the Government has, "by attacking … corporate reputation, achieved in substance an alteration of status." *Trifax*, 314 F.3d at 644. As Professor Hammond's expert report explains, that amounts to a deprivation of liberty, and the Commission may impose it, if at all, only after notice and a meaningful opportunity to be heard on the charges made. *See* Hammond Decl. 7-9.

Third, courts have consistently held that the Government deprives a business of liberty by debarring it—whether through "formal debarment" or through "broad preclusion, equivalent in every practical sense to formal debarment." *Trifax*, 314 F.3d at 643–44; *see, e.g.*, *Bank of Jackson County* v. *Cherry*, 980 F.2d 1354, 1358 (11th Cir. 1992) ("Federal circuit courts of appeals have … h[eld] that suspension or debarment of a government contractor … deprives the contractor of liberty"). Debarments deny companies the "right to follow a chosen trade." *Trifax*, 314 F.3d at 643. They also impose "stigma" and "alter [the debarred entity's] status in a tangible way." *Id.* at 644.

Under these cases, too, the labeling of a company as a "national security threat" and the exclusion of the company from the sale of equipment to USF recipients amounts to the deprivation of liberty. The effect is to debar the company from sales to federal funding recipients. Indeed, under the Commission's own regulations, the phrase "debarment" encompasses "any action … to exclude a person from activities associated with or relating to" universal-service support (47 C.F.R. § 54.8)—a capacious phrase that encompasses the selling of equipment to USF recipients. At a minimum, such an exclusion has a "practical" effect that is "equivalent" to a debarment; no

less than an official debarment, it precludes the company from selling its products to specified buyers.

To be sure, some debarment cases merely involve actions that preclude private entities from transacting with the Government, while the proposed rule would preclude private entities from transacting with other private entities who spend federal funds. But that makes no difference. The Due Process Clause requires more procedure, not less, when the Government restricts transactions between one "private business" and another than when it "manage[s] [its] internal operation[s]." *Cafeteria Workers* v. *McElroy*, 367 U.S. 886, 896 (1961). Thus, if debarring a company from transacting with the Government amounts to a deprivation of liberty, it follows *a fortiori* that debarring a company from transacting with the recipients of federal funds also amounts to a deprivation of liberty. For this reason, courts have understandably held that the due-process guarantee of a hearing also covers debarments of subcontractors—so that the Government must provide notice and a meaningful hearing before precluding a contractor (one private entity) from transacting with a subcontractor (another private entity). *Phillips* v. *Mabus*, 849 F. Supp. 2d 71, 87 & n.6 (D.D.C. 2012). A supplier of equipment to a USF recipient is similarly situated to a subcontractor; like the subcontractor, it sells products to an entity that in turn has a direct legal and economic relationship with the Government. So like the subcontractor, it too is entitled to notice and a meaningful hearing before debarment, if any, occurs.

2. The Due Process Clause requires that the company have an opportunity to review and respond to the evidence against it

"When the Constitution requires a hearing, it requires a fair one." *Wong Yang Sung* v. *McGrath*, 339 U.S. 33, 49 (1950). To determine what procedures are necessary for a hearing to be "fair," courts typically use the balancing test established in *Mathews* v. *Eldridge*, 424 U.S. 319

(1976). Under this framework, the procedures required turn on (1) "the private interest that will be affected," (2) the "risk of an erroneous deprivation of such interest" and "the probable value … of additional … procedural safeguards," and (3) "the Government's interest." *Id.* at 335. The Supreme Court and federal appellate courts have balanced these interests in a variety of cases involving national-security concerns. Each and every time, they have concluded that the Government must disclose the factual basis for its proposed action and give the party to be deprived of liberty a meaningful opportunity to rebut the Government's factual assertions.

Greene v. *McElroy*, 360 U.S. 474 (1959), illustrates this point. There, the Government sought to revoke a security clearance of a person who worked for a government contractor. The Supreme Court held that the Due Process Clause required the Government first to provide a hearing in which the individual had the opportunity to review and respond to the evidence asserted against him. Notwithstanding the Government's interests in protecting national security, it was required to obey the "immutable" principle that "the evidence used to prove the Government's case must be disclosed to the individual so that he has an opportunity to show that it is untrue." *Id.* at 496.

So too for cases in which the Government seeks to block a foreign entity's investment in the U.S. For instance, in *Ralls Corp.* v. *Committee on Foreign Investment*, 758 F.3d 296 (D.C. Cir. 2014), the President blocked a Chinese-owned company's investment in a windfarm in the U.S., on the ground that the acquisition posed a threat to U.S. national security. The D.C. Circuit held that, before the Government inflicts such a deprivation of property, "the evidence used to prove the Government's case must be disclosed … so that [the company] has an opportunity to show that it is untrue." *Id.* at 318.

Even suspected enemy combatants are entitled to more process than the Commission appears ready to give foreign-based technology companies such as Huawei. In *Hamdi* v. *Rumsfeld*,

542 U.S. 507 (2004), the Supreme Court held that due process entitles a suspected combatant to (at the very least) "notice of the factual basis" for the Government's decision and "a fair opportunity to rebut the Government's factual assertions before a neutral decisionmaker." *Id.* at 533 (plurality opinion). The Court acknowledged "the weighty and sensitive governmental interests in ensuring that those who have in fact fought with the enemy during a war do not return to battle against the United States." *Id.* at 531. Yet even these interests could not justify eroding the "essential constitutional promis[e]" of the right "to be heard" and to "rebut" the Government's factual assertions. *Id.*; *see id.* at 535 (underscoring that even "a state of war is not a blank check for the President when it comes to the rights of the Nation's citizens").

So too, the Commission proposes to give foreign-based technology companies less process than suspected foreign terrorist organizations. Before designating a group as a supposed foreign terrorist organization (thereby blocking its access to bank accounts), the Government must "notify [the group] of the unclassified material upon which [it] propose[s] to rely." *People's Mojahedin Organization* v. *Dep't of State*, 613 F.3d 220, 227 (D.C. Cir. 2010). The Government must also give the group the "opportunity to rebut the [evidence] or otherwise to negate the proposition that it is [a foreign terrorist organization]." *Id.*; *accord Nat'l Council of Resistance* v. *Dep't of State*, 251 F.3d 192, 209 (D.C. Cir. 2001) (due process requires giving the groups the opportunity "to rebut the administrative record or otherwise negate the proposition that they are foreign terrorist organizations").

These cases further establish that the fact that some of the Government's evidence is classified does not excuse the denial of a meaningful opportunity to respond to the Government's case. In such cases, "due process requires, at the least, that an affected party … be given access to the *unclassified* evidence on which the official actor relied and be afforded an opportunity to rebut

that evidence." *Ralls*, 758 F.3d at 319. And while the Government does not necessarily have to disclose the classified evidence to the affected party, it must disclose it "ex parte and in camera" to the reviewing court. *People's Mojahedin Organization*, 613 F.3d at 230. What is more, while the classified material may play a tangential role in the Government's decision, the D.C. Circuit has only ever upheld reliance on classified information where "the unclassified material provided to [the affected party] is sufficient to justify the [decision]." *Id.* at 231. The D.C. Circuit has cautioned that "none" of its cases suggest that "relying *critically* on undisclosed classified material would comport with due process." *Id.* (emphasis added); *see Fares* v. *Smith*, 249 F. Supp. 3d 115, 123 (D.D.C. 2017) ("the D.C. Circuit [has] suggested a limit to the ability of the government to rely on undisclosed, classified information … [where] the classified record [is] essential to uphold [the] designation").

These principles govern the matter at hand and foreclose the approach of the proposed rule. As Professor Hammond's expert report concludes, the Commission simply cannot label a company a "national security threat" and restrict purchase of its equipment without giving it notice and a fair hearing. *See* Hammond Decl. 3-9.

First, the private interests at stake here are at least as serious and profound as the private interests at stake in the cases just cited. The FCC proposes to brand companies "national security risks," to blacklist them and prohibit recipients of USF support from purchasing their equipment with such funds. For a company to be so deprived of the opportunity to do business "certainly is no small injury." *Joint Anti-Fascist Refugee Comm.* v. *McGrath*, 341 U.S. 123, 185 (1951) (Jackson, J., concurring). And the Government inflicts a "grievous loss" when it subjects a person to a "degrading" "label" or a "badge of infamy" (such as branding a company a "national security risk" that "'cannot be trusted'"). *Constantineau*, 400 U.S. at 436.

Second, the risk of erroneous deprivation here is at least as severe as in the cases cited above. There is a serious risk of "caprice" and "oppressive results" when a person is "not afforded a chance to defend itself" against allegations of being subject to "foreign influence" and posing a threat to "national security." *Id.* at 437. History has taught that concerns about national security can provoke anxiety, passion, risk-aversion, nationalism, and, in some cases, even xenophobia and bigotry. *See, e.g.*, *Dennis v. United States*, 341 U.S. 494 (1951); *Korematsu* v. *United States*, 323 U.S. 214 (1944); *Debs* v. *United States*, 249 U.S. 211 (1919); Aliens Act, 1 Stat. 570 (1798). In such circumstances, there are obvious risks that officials will overlook the company's evidence of its independence from the alleged "foreign state influence." NPRM, ¶ 5. There is also a risk that officials will overlook arguments that the evidence on which they rely is untrustworthy or unreliable. And there is obvious potential for unfounded hyperbole, exaggeration, bias, and hysteria—not to mention political gamesmanship and showmanship. Indeed, the chain of events that was set off by the 2012 HPSCI Report perfectly illustrates these problems. As discussed in Sections II.C above and VII below, because Huawei has not been afforded an adequate opportunity to present evidence that rebuts any specific allegations, it has suffered from capricious labels being attached to it based on rumor, innuendo, and scattered media reports. As these facts demonstrate, the risk of erroneous deprivation from lack of meaningful hearing procedures and the opportunity to submit and confront evidence is exceedingly high in this context.

Third, the Government's interest is no weightier here than in the cases just discussed. Courts have required giving the affected party the opportunity to rebut the Government's evidence even in cases involving war and terrorism. This case does not involve anything like that; it involves, instead, vague assertions of "national security risks" associated with "foreign state influence." And it involves telecommunications funding for libraries, low-income rural areas, and the

like—which are not exactly hotbeds of foreign intelligence activity and U.S. security interests. Before branding a company as a threat to national security and disqualifying it from supplying products to USF recipients, the Commission must obey the "immutable" principle that "the evidence used to prove the Government's case must be disclosed to the individual so that he has an opportunity to show that it is untrue." *Greene*, 360 U.S. at 496. If this principle holds true in the context of enemy combatants who literally have taken up arms against the U.S., surely it holds true in the context of telecommunications companies that happen, for example, to have their headquarters in China.

Finally, Congress itself has deemed similar procedural safeguards essential in other contexts. "When the Constitution requires a hearing, it requires a fair one, one before a tribunal which meets at least currently prevailing standards of impartiality." *Wong Yang Sung*, 339 U.S. at 50; *see Burnham v. Superior Court*, 495 U.S. 605, 627 (1990) (opinion of Scalia, J.) ("both past and current practice" guide due-process analysis). As Professor Hammond's expert report shows, "currently prevailing standards of impartiality," reflected in legislation enacted by Congress, require agencies ranging from the Department of Commerce and the Federal Energy Regulatory Commission to the General Services Administration and the Office of Management and Budget to provide a formal hearing before disadvantaging a company on the basis of national-security concerns. *See* Hammond Decl. 9-14. The Due Process Clause requires the Commission to obey *at least* the same standards.

B. The Communications Act and the APA Also Guarantee the Company the Opportunity to Respond to the Evidence Against It

The Communications Act and the APA also require the Commission, at the constitutionally mandated hearing, to disclose the factual basis for any designation of a company as a national-

security risk, and to give the company an appropriate opportunity to rebut those factual assertions, at the constitutionally required hearing.

1. Communications Act

The Communications Act evinces an acute concern about affording robust procedural protections to individuals affected by the Commission's actions. It sets out certain procedural requirements that apply "in *every* case of adjudication … designated by the Commission for hearing." § 409(a)–(c) (emphasis added). Even if the Commission were authorized to make national-security judgments in the USF context— which it is not (see Section III above) —the Due Process Clause would require the Commission to "designat[e] … for a hearing" a proposed decision to label a company a "national security threat" and to restrict its market access. That hearing would qualify as an "adjudication"; § 409(a) defines "adjudication" by cross-reference to the APA, which, in turn, defines that term as "any agency process for the formulation of an order." The Communication Act's procedural requirements thus apply here; under the statute's plain text ("*every* case of adjudication"), it makes no difference whether the Commission holds the hearing by constitutional compulsion, by statutory compulsion, or voluntarily.

Indeed, the Commission plainly understands that the statute's procedural protections must be afforded to an entity before it may be excluded from activities associated with the USF. Under the Commission's debarment regulation, the agency must, before excluding an entity from "activities associated with or relating to" universal service-funding, disclose the factual basis for the debarment and give the affected party an opportunity to respond. 47 C.F.R. § 54.8.

There is no valid reason for affording fewer procedural protections where the blacklisting applies to the company that supplies equipment to the USF recipient rather than to the USF recipient itself. In either case, the purposes of a hearing requirement—providing process to adversely affected individuals and protecting against risk of factual error—are equally at stake.

Under the Communications Act's pertinent procedural provisions, the person conducting the hearing must "prepare and file an initial, tentative, or recommended decision." § 409(a). The affected party must then have the opportunity "to file exceptions and memoranda in support thereof." § 409(b); *see also* § 409(c)(1) (further specifying notice requirements).

The "recommended decision" must disclose the facts on which the Commission proposes to rely. There would be no point to requiring the agency to file a recommended decision, and allowing the affected party to respond, if the recommended decision could just be an empty piece of paper that omits "the facts and the law." *See id.* The statutory requirement has meaningful effect only if the recommended decision sets out the relevant legal and factual determinations, to which the party can then respond. Anything else would be a charade.

Indeed, the Communications Act copies the "recommended decision" procedure from the APA. *See* 75 Stat. 420 (1961) (amending the Communications Act to add the relevant terms of § 409 around a decade after the enactment of the APA). Whereas the APA requires a recommended decision only for formal adjudications (*see* 5 U.S.C. § 557(c)), the Communications Act, as just discussed, extends these requirements to *all* adjudications. The APA, in turn, explicitly requires recommended decisions to include "findings and conclusions, and the reasons or basis therefor, on all material issues of fact, law, or discretion." § 557(c)(3)(A). By parroting the phrase "recommended decision" from the APA, the Communications Act also imports these requirements regarding what a recommended decision must contain. *See T-Mobile South, LLC* v. *City of Roswell*,

135 S. Ct. 808, 815 (2015) ("When Congress employs a term of art, it presumably knows and adopts the cluster of ideas that were attached to each borrowed word in the body of learning from which it was taken.").

The Communications Act also enshrines additional procedural protections that are designed to produce a fair, trustworthy, and accurate fact-finding process. For example, the statute specifies that the entity that rules upon the exceptions filed by the affected party either will be "the Commission" or "the authority within the Commission, if any, to whom the function of passing upon the exceptions is delegated." In the latter case—that is, in the case of a delegation of such authority—the statute further guarantees that the official who "pass[es] upon the exceptions" filed by the affected party "shall not be the same authority which made the decision to which the exception is taken." § 409(b). This procedural protection ensures a neutral decisionmaker.

2. Administrative Procedure Act

Indeed, because the requirement of a hearing arises from the Due Process Clause, the APA's formal-adjudication procedures—which go beyond the procedures required by the Due Process Clause and Communications Act—apply, if the Commission is authorized to adjudicate national security issues at all. Under the APA, an agency must use a formal-adjudication procedure "in every case of adjudication required by statute to be determined on the record after opportunity for an agency hearing." § 554(a). The Supreme Court has held that these formal-adjudication procedures are triggered when a hearing is compelled by the Due Process Clause. *Wong Yang Sung*, 339 U.S. at 49.

"The constitutional requirement of procedural due process of law derives from the same source as Congress' power to legislate and, where applicable, permeates every valid enactment." *Id.* As a result, "the limitation to hearings 'required by statute' … exempts … only those hearings

which administrative agencies may hold by regulation, rule, custom, or special dispensation; not those held by compulsion." *Id.* After all, one "would hardly attribute to Congress a purpose to be less scrupulous about the fairness of a hearing necessitated by the Constitution than one granted by it as a matter of expediency." *Id.* at 50. The Supreme Court reached these conclusions nearly 70 years ago, but they remain good law today. *See, e.g.*, *United States* v. *Mead Corp.*, 533 U.S. 218, 243 (Scalia, J., dissenting) (2001) (citing *Wong Yang Sung*, without disagreement from the majority, for the proposition that an agency must use "formal adjudication procedures" where a hearing is "prescribed … either by statute or by the Constitution"); *Collord* v. *U.S. Dep't of Interior*, 154 F.3d 933, 936 (9th Cir. 1998) ("According to *Wong Yang Sung*, hearings necessitated by the Constitution are included in the scope of hearings that are covered by § 554 of the APA").

The APA requires that the subject of the adjudication receive notice of "the time, place, and nature of the hearing," "the legal authority" under which the hearing is to be held, and "the matters of fact and law asserted." § 554(b). The party must have the opportunity to present "facts" and "arguments." § 554(c). It is also "entitled to present [its] case or defense by oral or documentary evidence, to submit rebuttal evidence, and to conduct such cross-examination as may be required for a full and true disclosure of the facts." § 556(d). The Commission must make its decision on the record; it may not receive or rely on "ex parte communication[s] relevant to the merits of the proceeding." § 557(d)(1)(B). Only after a proceeding satisfying all of these requirements could the Commission, if at all, label a company a "national security threat" and preclude the use of USF funds to buy that company's equipment.

C. The Proposed Rule Unlawfully Disregards These Constitutional and Statutory Procedural Requirements

The proposed rule fails to comply with the constitutional and statutory principles just discussed. Contrary to elementary due-process principles, the Commission apparently proposes to blacklist manufacturers without any hearing at all (much less a meaningful one). Contrary to the Communications Act, the Commission apparently proposes to deny a blacklisted company the opportunity to see the evidence against it and to respond. Contrary to the APA, it apparently proposes to subject companies to blacklisting without providing a formal adjudication and attendant safeguards (such as the opportunity to present the company's case, to rebut the Government's evidence, and, where appropriate, to cross-examine witnesses). And, as Professor Hammond's expert report demonstrates, the Commission proposes to disregard conventional practice and legal norms that apply when agencies make determinations such as the ones that the Commission contemplates here. Hammond Decl. 2, 8-17 (discussing applicable constitutional and statutory requirements, "contemporary norms of procedure," and "the unusual nature of the FCC's proposed approach").

Instead, the NPRM apparently proposes three procedural shortcuts: (1) the Commission or another agency could use rulemaking to issue a list of companies that supposedly raise national-security concerns; (2) the Commission could define a company as a national-security risk if an existing statute bars that company from providing equipment to the Federal Government for national-security reasons; or (3) the Commission could define a company as a national-security risk if another agency has barred the company from providing equipment to the Federal Government for national-security reasons.

But none of these alternatives cures the due-process, Communications Act, and APA defects just discussed. Quite the opposite, these alternatives entail new constitutional and statutory violations of their own.

1. Neither the Commission nor another agency may use rulemaking to issue a list of blacklisted companies

Under one "possible approach" contemplated in the NPRM, either the Commission itself or "a federal agency other than the Commission" would, seemingly through rulemaking, create a "list of companies" or "criteria" for creating a list of companies that "raise national security concerns." NPRM ¶¶ 20, 22. Regardless of whether this approach involves the promulgation of an explicit blacklist or the adoption of "criteria" then applied by the agency without providing an individualized hearing on the charges, it is legally impermissible.

First, the use of rulemaking to create such a blacklist would violate the Due Process Clause. As Professor Hammond explains in her expert report, the Due Process Clause allows an agency to use rulemaking to adopt general policies that affect the liberty of a large group of people, but not particularized policies that affect the liberty of a small group of people. *See* Hammond Decl. 4 & n.11. This distinction reflects the reality that particularized decisions pose a greater threat to liberty than does general policymaking. This distinction follows from two Supreme Court cases, *Londoner* v. *Denver*, 210 U.S. 373 (1908), and *Bi-Metallic Investment Co.* v. *State Board of Equalization*, 239 U.S. 441 (1915). In *Londoner*, the Court held that due process required individualized process before a state agency valued a particular landowner's land for tax purposes. 210 U.S. at 385. In *Bi-Metallic*, by contrast, the Court held that due process did not require individualized process before a state agency increased the valuation of all taxable property in an entire city. 239 U.S. at 445–46. These cases, together, stand for the proposition that an administrative agency may

constitutionally forgo adjudication when adopting a "general" "rule of conduct," but not when "a relatively small number of persons [is] concerned, who [are] exceptionally affected, in each case upon individual grounds." *Id.* at 446.

"The framers of the Constitution knew, and we should not forget today, that … nothing opens the door to arbitrary action so effectively as to allow … officials to pick and choose only a few to whom they will apply legislation and thus to escape the political retribution that might be visited upon them if larger numbers were affected." *Ry. Express Agency* v. *New York*, 336 U.S. 106, 112 (1949) (Jackson, J., concurring); *see INS* v. *Chadha*, 462 U.S. 919, 966 (1983) (Powell, J., concurring in the judgment) ("[Government] is most accountable politically when it prescribes rules of general applicability. When it decides rights of specific persons, those rights are subject to the tyranny of a shifting majority"); *Plaut* v. *Spendthrift Farm, Inc.*, 514 U.S. 211, 246 (1995) (Breyer, J., concurring in the judgment) ("generality [is] a characteristic that helps avoid the problem of legislatively singling out a few individuals for adverse treatment"); *Coniston Corp.* v. *Village of Hoffman Estates*, 844 F.2d 461, 469 (7th Cir. 1988) ("A statute, unlike a judicial decision, applies directly to a whole class of people, and it is this attribute that makes democratic checking feasible, though it is far from perfect. The smaller the class affected by a nominally legislative act, the weaker the democratic check.").

The general-particular distinction, drawn over a century ago, remains the law of due process today. *See United States* v. *Florida East Coast Ry.*, 410 U.S. 224, 245–46 (1973) ("The basic distinction between rulemaking and adjudication is illustrated by … *Londoner* … [and] *Bi-Metallic* … Later decisions have continued to observe the distinction"); *Minnesota State Bd. for Community Colleges* v. *Knight*, 465 U.S. 271, 284 (1984) ("Executive agencies [may] make policy decisions of widespread application without … individual argument"); *Safari Club Int'l* v. *Zinke*, 878 F.3d

316, 332 (D.C. Cir. 2017) (repeating the "basic distinction" between *Londoner* and *Bi-Metallic*"). Moreover, "judicial constructions of a 'rule' under the APA follow these precepts." *Safari Club*, 878 F.3d at 332. Even though the APA defines "rule" to include statements of "particular applicability," agencies must still provide individualized hearings where "a particularized [deprivation of liberty] affect[s] particular [people] in each case upon individual grounds." *Id.*; *see Vermont Yankee Nuclear Power Corp. v. Natural Res. Def. Council, Inc.*, 435 U.S. 519, 542 (1978) ("In prior opinions we have intimated that even in a rulemaking proceeding when an agency is making a quasi-judicial determination by which a very small number of persons are exceptionally affected, in each case upon individual grounds, in some circumstances additional procedures may be required in order to afford the aggrieved individuals due process."); Hammond Decl. 4 & n.11.

Under these due-process principles, neither the FCC nor any other agency may use rulemaking to frame a list of companies that are to be branded "national security threats" and barred from selling equipment to USF recipients. This designation would affect "a relatively small number of persons," *Bi-Metallic*, 239 U.S. at 446; the NPRM, indeed, contemplates that it could affect as few as three companies (Huawei, ZTE, and Kaspersky Lab). NPRM, ¶ 4. These companies would be "exceptionally affected," *Bi-Metallic*, 239 U.S. at 446; these companies, and no others, would be declared threats to the nation's security and would be denied the opportunity to sell their products to funding recipients. And these companies would be affected on "individual grounds," *id.*; the basis for the deprivation of liberty is that the particular "company" supposedly "pos[es] a national security threat." Proposed Rule, 49 C.F.R. § 54.9. An individualized adjudication is thus required; a rulemaking does not suffice.

Second, the use of rulemaking to create such a blacklist would violate the Bill of Attainder Clause, which provides that "No Bill of attainder … shall be passed." U.S. Const. art. I, § 9, cl 3.

"A bill of attainder is a legislative act which inflicts punishment without a [hearing]." *United States* v. *Lovett*, 328 U.S. 303, 315 (1946). A rule made by an agency is a "legislative act" for these purposes. When an executive agency exercises rulemaking authority, it "acts … quasi legislatively." *Humphrey's Ex'r*, 295 U.S. at 628; *Whitman*, 531 U.S. at 488 (2001) (Stevens, J., concurring in part) ("agency rulemaking authority is 'legislative power'"); *City of Arlington* v. *FCC*, 569 U.S. 290, 312 (2013) ("Although modern administrative agencies fit most comfortably within the Executive Branch, as a practical matter they exercise legislative power, by promulgating regulations with the force of law"). These quasi-legislative acts are subject to the restrictions imposed by the Bill of Attainder Clause. *See Joint Anti-Fascist Refugee Comm.*, 341 U.S. at 144 (Black, J., concurring) ("I cannot believe that the authors of the Constitution, who outlawed the bill of attainder, inadvertently endowed the executive with power to engage in the same tyrannical practices that had made the bill such an odious institution."); *Dehainaut* v. *Pena*, 32 F.3d 1066, 1071 (7th Cir. 1994) ("We stated [in an earlier case] that an administrative rule adopted pursuant to Congressionally delegated authority must be viewed as tantamount to a statute for the purpose of … the *ex post facto* clause … Having gone this far, it is a conceivable step to also view an agency policy … as the functional equivalent of a legislative enactment for bill of attainder purposes."); *cf. Federal Maritime Comm'n* v. *S.C. State Ports Auth.*, 535 U.S. 743, 758 (2002) (holding that the doctrine of state sovereign immunity applies to agency adjudications, even though such adjudications technically involve exercises of executive rather than judicial power, because an adjudication "walks, talks, and squawks very much like a lawsuit").

A rule that labels a listed group of companies as threats to national security, barring them from selling their products to federal funding recipients, also imposes "punishment" for these purposes. "The very specificity of the [rule]"—which, according to the NPRM, could apply to as few

as three companies—"would mark it as punishment, for there is rarely any valid reason for such narrow legislation." *Nixon* v. *Adm'r of Gen. Servs.*, 433 U.S. 425, 485 (1977) (Stevens, J., concurring); *see also id.* at 486 ("[an] otherwise nonpunitive statute [can be] made punitive by its specificity"). Moreover, "officially prepared and proclaimed blacklists" inherently impose punishment and thus "possess almost every quality of [classic] bills of attainder." *Joint Anti-Fascist Comm.*, 341 U.S. at 144 (Black, J., concurring). "Our basic law … wisely withheld authority for resort to executive investigations, condemnations and blacklists as a substitute for imposition of legal types of penalties … in accordance with procedural safeguards of the Bill of Rights." *Id.*; *see also Richmond* v. *J.A. Croson, Co.*, 499 U.S. 469, 513 (1989) (Stevens, J., concurring in the judgment) ("Legislatures are primarily policymaking bodies that promulgate rules to govern future conduct. The constitutional prohibitions against the enactment of *ex post facto* laws and bills of attainder reflect a valid concern about the use of the political process to punish or characterize past conduct of private citizens.").

Third, the use of rulemaking to create a blacklist would violate the APA. The APA prohibits rules that have "unreasonable secondary retroactivity"—in other words, rules that change the "legal consequences of past actions" in a way that undermines "reliance upon the pre-existing rule." *Bowen* v. *Georgetown Univ. Hosp.*, 488 U.S. 204, 219–20 (1988) (Scalia, J., concurring); *see U.S. AirWaves, Inc.* v. *FCC*, 232 F.3d 227, 233 (D.C. Cir. 2000) ("A secondarily retroactive rule is valid only to the extent that it is reasonable."). The proposed rule would have unreasonable secondarily retroactive effects. Companies such as Huawei have made substantial investments in reliance on their ability to sell their products to recipients of USF funding and, more importantly, to other companies in the U.S. and around the world. Yet the proposed rule, if applied to companies such as Huawei, would have the legal effect of prohibiting them from selling their products to the

funding recipients, and the practical effect of preventing them from selling their products to many others. In addition, the proposed rule would likely undermine "multiyear contracts" and "contracts with voluntary extensions." NPRM, ¶ 18. These effects are unreasonable.

Finally, to the extent that the Commission assigns the task of compiling the blacklist to another agency, such outsourcing would constitute an unlawful subdelegation. When a federal statute "delegates authority to a federal … agency," the agency may "subdelegat[e]" that authority, if at all, only to "a subordinate." *U.S. Telecom Ass'n* v. *FCC*, 359 F.3d 554, 565 (D.C. Cir. 2004). The agency may *not* subdelegate that authority to "an outside party" (whether "private or sovereign"). *Id.* at 565–66. "This distinction is entirely sensible. When an agency delegates authority to its subordinate, responsibility—and thus accountability—clearly remain with the federal agency. But when an agency delegates power to outside parties, lines of accountability may blur, undermining an important democratic check on government decision-making." *Id.* at 565. These principles preclude the Commission from passing off the task of compiling a list of blacklisted companies to a different federal agency, an "outside party" that is in no sense "subordinate" to the Commission.

2. The Commission may not designate a company as a national-security risk on the basis of existing statutes restricting the company's ability to provide equipment or services

Under the second alternative identified by the NPRM, the Commission would define a company as a national-security risk if "existing statutes" bar that company "from providing certain equipment or services to federal agencies for national security reasons." NPRM, ¶ 21. The NPRM identifies only one such "existing statute": the 2018 NDAA. *Id.* But this approach, too, is unlawful. Indeed, even placing significant reliance on the statute, or establishing a "criterion" that is based on a list in some other (undefined) statute, is impermissible.

First, treating an existing statute as a substitute for a hearing would deny due process. The Due Process Clause, as already discussed, requires the Commission to hold a hearing before it designates a specific company as a national-security risk (if such a designation were even permissible, which it is not). Existing statutes do not fulfill the constitutional requirement; the enactment of a statute is not the provision of a constitutionally necessary individualized hearing. *See Londoner*, 210 U.S. at 385.

Second, piggybacking on the 2018 NDAA would violate the 2018 NDAA itself. That statute imposes a narrow restriction on listed telecommunications companies: the Department of Defense may not use equipment made by certain telecommunications providers to carry out its "nuclear deterrence mission" and its "homeland defense mission." § 1656. By necessary implication, the Department may use those companies' equipment for any other program. *See, e.g.*, *Cipollone v. Liggett Grp., Inc.*, 505 US 504, 517 (1992) (statute expressly preempting state laws as to specific matters necessarily implies that laws outside that scope are not preempted); *EchoStar Satellite L.L.C. v. FCC*, 704 F.3d 992, 999 (D.C. Cir. 2013) (statute expressly authorizing the Commission to regulate cable systems implied a lack of authority to impose such regulations on other categories of video programming distributors). The Commission has no authority to expand the NDAA's restriction to cover other programs administered by other agencies. That is so because, in the fields of national security and foreign policy, the legal consequences that attach to particular actions are exclusive—so that other governmental bodies may not attach additional consequences of their own. *See Arizona* v. *United States*, 567 U.S. 387, 402 (2012) (states may not impose their own punishments for violations of federal immigration law). That is particularly so here, given the specificity of the 2018 NDAA: it restricts the Defense Department's ability to use the listed companies' equipment only when carrying out two particular missions, and it imposes no restrictions

at all on other federal agencies. The 2018 NDAA thus strikes a careful balance between supposed national-security concerns on the one hand and (for instance) avoiding international discord on the other. The Commission has no power to upset that balance by adding consequences of its own to those specified in the statute.

Third, reliance on the 2018 NDAA would be arbitrary and capricious, as explained in Section IV.B.3 above. The Commission acts arbitrarily by assuming that, just because Congress concluded that a particular company's equipment is supposedly too risky for a ballistic-missile facility, the same equipment must also be too risky for an elementary school.

3. The Commission may not designate a company as a national-security risk on the basis of another agency's decision to debar the company

Alternatively, the NPRM proposes defining a company as a national-security risk if "any agency of the Federal Government" has, "for reasons of national security," "prohibited [the company] from bidding on a contract, participating in an auction, or receiving a grant." NPRM, ¶ 20. But this approach is likewise unlawful.

First, abdicating responsibility to other agencies violates the APA. Under that statute, the Commission must use "reasoned decisionmaking" in making any determination. *State Farm*, 463 U.S. at 52. As part of this APA-mandated decisionmaking process, "the agency itself" must "examine the relevant data." *Id.* It must consider every "important aspect of the problem," while refraining from "rel[ying] on factors which Congress has not intended it to consider." *Id.* at 43. Then, it must "articulate a satisfactory explanation for its action." *Id.* The agency must itself comply with these requirements; nobody else may "supply a reasoned basis for the agency's action that the agency itself has not given." *Id.*

The Commission's proposed approach violates these fundamental principles of administrative law. In treating another agency's decision as conclusive, the Commission would *not* examine the relevant data. It would *not* consider every important aspect of the problem. And it would *not* articulate its own explanation for the action. Instead, the Commission would merely parrot the actions of some other agency, without any reasoned explanation for the choice to do so. This approach reduces the agency from a reasoned decisionmaker to a ventriloquist's puppet.

Second, treating another agency's decision as conclusive would violate the principle that preclusion covers only the issues actually decided in the original proceeding. The preclusive effect of agency decisions is generally governed by the "same … rules, … subject to the same exceptions and qualifications," as the preclusive effect of "a judgment of a court." *B & B Hardware, Inc.* v. *Hargis Indus., Inc.*, 135 S. Ct. 1293, 1303 (2015). One of those rules is that an agency's decision is "conclusive" only with respect to "an issue of fact or law [that] is actually litigated and determined." *Id.* at 1303. Indeed, the Due Process Clause requires this limitation on the scope of preclusion. *Fayerweather* v. *Ritch*, 195 U.S. 276, 298–99 (1904).

The Commission's proposed approach contravenes these long-established preclusion rules. In any earlier proceeding, the other agency would at most have "actually determined" that the company's participation *in that agency's programs* would pose a risk to national security. The issue before the Commission, however, would be quite different: whether the company's provision of equipment *to USF recipients* would pose a risk to national security. Similarly, in any earlier proceeding, the other agency would at most have "actually determined" that the company posed a risk to national security *at that time*. The proposed rule, however, turns on whether the company's equipment threatens national security "going forward." NPRM, ¶ 2. A determination by the Department of Defense that a company's equipment posed a risk to nuclear-launch facilities five years

ago is far from the same thing as a determination that the equipment also poses a risk to rural libraries today and in the future. Further, the only consequence at stake in that earlier proceeding would have been debarment from that agency's programs. The parties would have had no reason to litigate that earlier proceeding with the expectation that it would also carry the consequence of debarment from selling equipment to USF recipients.

Third, treating another agency's decision as conclusive would violate the principle that a proceeding is entitled to preclusive effect only if the party to be bound had the opportunity to be heard in that earlier proceeding. Under the common law of preclusion, preclusion is appropriate only if the party "had an adequate opportunity to litigate" its case in the initial proceeding. *B & B Hardware*, 135 S. Ct. at 1303. Moreover, applying preclusion in the absence of such an opportunity would be "inconsistent with the due process of law." *Taylor* v. *Sturgell*, 553 U.S. 880, 897 (2008).

The Commission's proposed approach contravenes these rules. It would give binding effect to another agency's debarment decision even if that agency gave the blacklisted company *no* opportunity (let alone an adequate opportunity) to be heard. It would also do so even if the blacklisted company had no opportunity to seek judicial review in the previous proceeding, which is an essential component of the "adequate opportunity to litigate," *see* Restatement (Second) of Judgments § 28(1).

Finally, even placing significant reliance on such decisions by other agencies would be arbitrary and capricious. To repeat, an agency acts arbitrarily and capriciously (and thus unlawfully) by failing to rest its decision on "the relevant factors" or by failing to articulate a "rational connection between the facts found and the choice made." *State Farm*, 463 U.S. at 43. There is no "rational connection" between another agency's past decision to exclude a particular company from its programs on national-security grounds, and the Commission's decision to exclude that

company from activities associated with the USF going forward. For one, as already discussed, the degree of sensitivity to national-security risks differs dramatically from one context to the other; a rational Government would be less tolerant of national-security risks when dealing with a ballistic-missile facility than when dealing with a rural library. For another, as discussed above, the other agency's decision will have turned on whether the blacklisted company posed a risk to national security at the time of that decision, not on whether it continues to pose such a risk now.

VII. THE PROPOSED RULE RELIES ON UNVERIFIED AND UNSUPPORTABLE FACTUAL ALLEGATIONS AGAINST HUAWEI

Although, as discussed earlier, the proposed rule does not purport to designate any specific company as a "threat to national security," the text of the NPRM as well as the context surrounding it makes it obvious that the Commission's real intention is to designate Huawei, along with one or two other companies, as such a "threat" as soon as possible after adopting a rule. Besides the Constitutional and legal obstacles to such a designation by fiat discussed previously, the Commission's rush to blacklist Huawei based on unverified, unproven, and indeed unspecified allegations in the absence of any substantial evidence is arbitrary and capricious.

A. Equipment Sold by Huawei in the United States Poses No Threat to National Security

There is no evidence whatsoever (and the NPRM cites none) that any equipment manufactured by Huawei, or sold by it in the United States or anywhere else in the world, has ever posed any national security risk. Huawei equipment is widely used in over 170 countries across the world—including close U.S. allies such as the U.K.—without undermining any nation's security. Dowding Decl. ¶ 7. Huawei equipment has passed many well-recognized security certifications including ISO 27001, ISO 9001, ISO 28000, ISCCC, C-TPAT, Common Criteria, CSA STA, PA

DSS, OTTPS, FIPS 140-2, and ePrivacy Seal. Suffolk Decl. 8-10; *see also* Exhibit O, Certification and Testing of Huawei Products.

There is no evidence that Huawei equipment has ever included any code at the behest of the Chinese government, any backdoor, or any malicious code, or posed a national security risk in any way. As discussed in more detail below, no credible source has ever claimed to have actual knowledge of any malware's existence, and Huawei emphatically denies that it ever has, or would, tamper with its equipment or software at the behest of the Chinese government.

Of course, the Commission might assert that its proposed action is based on the *potential* for *future* harmful actions by Huawei, despite the absence of any such conduct in the past. But such a speculation itself would have to be based upon some rational, factual basis to survive judicial review. At least theoretically, *any* company, no matter how spotless its past record, could be infiltrated in the future by some hostile element and thereby pose a threat to the national security, but the Commission must be able to articulate some factual basis for concluding that a company on its blacklist poses a specific future threat that other companies do not. Otherwise, it would fall afoul of the most basic principles of administrative law discussed in Section IV above.

Contrary to speculation in the 2012 HPSCI Report, Chinese law does not give the government unfettered authority to interfere in the operations of Huawei, a privately owned and operated company. Under Chinese law, private enterprises are legally independent of the Chinese government. Exhibit D, Declaration of Ariel Ye ("Ye Decl.") at ¶¶ 9-15. No law permits the Chinese government or Chinese public servants to interfere with a private company's operations or business decisions. *Id.*; *see also* Chen & Fang Decl. ¶¶ 84-85. Moreover, Chinese law protects companies by providing legal remedies where a company's "autonomy in business management" has been infringed. Ye Decl. ¶¶ 31-34. This is consistent with the Constitution of China as well as case

precedent, in which the Supreme People's Court of China has upheld "the inviolable right of companies to manage their own affairs." *Id.* at ¶¶ 35-41. Even the Rules and Code of Conduct of the Chinese Communist Party recognize that Chinese law "protects the rights of enterprises' autonomy of operation" and lays out penalties for any persons responsible for "interference in the autonomy of the people in production and management." *Id.* at ¶¶ 55-58 (citing Chinese Communist Party Disciplinary Regulations (rel. Oct. 21, 2015), Article 106; Decision of the Central Committee of the Communist Party on Several Major Issues Concerning Ruling the Country in Accordance of Law, 4th Plenary Session of the 18th Central Committee of the Chinese Communist Party of China (Oct. 23, 2014)).

Huawei enjoys the full protection of Chinese law, in furtherance of economic freedom, to operate and manage itself autonomously. *Id.* at ¶¶ 59-67. In addition, specific legislation governs Shenzhen, the city where Huawei is located, which has been designated as a Special Economic Zone. *Id.* at ¶¶ 26-27, 66-67. Shenzhen's pro-business regulations and free economy ideals make unlawful interference with private companies particularly rare in the area. *Id.*

China's national security laws have also been misunderstood by U.S. government agencies. For example, the 2012 HPSCI Report expressed concern about a provision of the former State Security Law that appeared to allow the Chinese government access to telecommunications operators' equipment, which has since been superseded by the Counterespionage Law of 2014. But this law is targeted at relevant organizations and individuals of China related to the specific purpose of counterespionage work, not a telecommunications equipment manufacturer or its overseas subsidiaries. Chen & Fang Decl. ¶¶ 11-21, 24. In general, Chinese laws regarding cooperation with law enforcement and security agencies apply to telecommunications and information service providers, not to equipment manufacturers; and they do not apply to overseas subsidiaries of these

entities. Moreover, none of these laws allow the Chinese government or its officials to require telecommunications equipment manufacturers to plant backdoors or spyware into telecommunications equipment. *Id.* at ¶¶ 42-46, 65-66, 80-82. Huawei equipment sold in the U.S. is sold through Huawei USA, which is headquartered in Plano, Texas, and governed by U.S. law—not by its Chinese parent company or Chinese law. Dowding Decl. ¶¶18-20. Huawei USA does not offer any services to end user consumers of telecommunications services in the United States, only to the companies that purchase its telecommunications equipment. *Id.* at ¶ 22. Although Huawei USA purchases equipment from its parent company for import into the U.S. for sale to Huawei USA customers, it complies with all applicable U.S. laws with respect to that equipment—and Huawei USA, not its parent company, is responsible for servicing equipment deployed in the U.S. *Id.* at ¶¶ 22-24.

B. The Rationale Stated in the NPRM Provides No Basis to Designate Huawei as a Potential Threat to National Security

It would be arbitrary and capricious for the FCC to designate Huawei as a potential threat to national security based upon nothing more than the unsupported suspicions and innuendo cited in the NPRM as the basis for opening this proceeding. The documents cited in the NPRM and in separate statements by Commissioners, some of which are over five years old, do not identify any specific threat arising from Huawei—or any other named company—but merely cast aspersions based on the location of the company's headquarters and the nationality of its founder.

The NPRM cites a variety of documents and sources in an effort to justify the Commission's proposal, but none provides a basis for acting specifically against Huawei. The Executive Branch documents cited in paragraph 3 of the NPRM—such as Executive Order 13800 and Pres-

idential Policy Directive 21—undoubtedly support the notion that security of communications infrastructure is an important policy concern, but none establishes any basis for labeling Huawei as a threat to national security.

Paragraph 4 of the NPRM cites, and discusses in some detail, the 2012 HPSCI Report that specifically focused on Huawei and ZTE, heavily emphasizing their alleged "connections to the Chinese government," and recommended avoiding the use of either company's products in U.S. telecommunications networks. NPRM, ¶ 4 (quoting 2012 HPSCI Report at iv). The 2012 HPSCI Report, however, did not cite any evidence of a specific threat, but rather concluded that Huawei had not proved to the Committee's satisfaction that it was not a threat. Setting aside the inherent difficulty in proving a negative, Huawei provided the committee with extensive evidence which it failed to consider—and then failed to cite any concrete proof for its allegations. It is clear that the committee targeted Huawei because of its Chinese origin, and not because of any specific actions or omissions by the company. The 2012 HPSCI Report was based on rumor and speculation, and designed to achieve a predetermined outcome dictated by politics rather than national security. This report, which has no legal force or effect, should not be given any weight by the Commission given the lack of any supporting evidence for its recommendations and conclusions. *See Safe Extensions, Inc. v. FAA*, 509 F.3d 593 (D.C. Cir. 2007) (holding that an agency must have evidence to support its assertions and that its own conclusions are not evidence).

The letter from 18 Senators and Representatives to Chairman Pai, cited in paragraph 5 of the NPRM, is an even less persuasive basis for Commission action, as it simply repeats the now five-year-old allegations of the 2012 HPSCI Report without providing any new information. Although Huawei has continued to offer its products for sale in the U.S. since 2012, neither HPSCI nor any of the Members of Congress who wrote to Chairman Pai have even suggested, let alone

shown as fact, that the use of this equipment has caused any harm or risk to the national security in any way. While the absence of any incident over more than five years is not conclusive proof, it certainly is suggestive that the concerns expressed in the 2012 HPSCI Report were hyperbolic and unjustified.[23] This political rhetoric is not the kind of "substantial evidence" required to justify Commission action (*see* 5 U.S.C. § 706(2)(E)); instead, it is insubstantial and lacking in evidentiary value.

[23] The November 10, 2010, letter from Rep. Anna Eschoo to then-Chairman Genachowski, cited in footnote 9 of the NPRM, carries no more weight. That letter makes unjustified and unsupported claims about a supposed close relationship between Huawei and the Chinese army, apparently based on the fact that the founder of Huawei is a veteran who served in his country's armed service. It also complains about a supposed lack of "corporate transparency," but offers no facts to back up this claim.

VIII. CONCLUSION

For the foregoing reasons, the Commission should not adopt the proposed rule, and should terminate this rulemaking proceeding. Adoption of the proposed rule would be contrary to the Constitution, would exceed the Commission's jurisdiction under the Communications Act, and would be arbitrary and capricious.

Respectfully submitted,

Glen D. Nager
Bruce A. Olcott
Ryan J. Watson
Vivek Suri
JONES DAY
51 Louisiana Ave, NW
Washington, D.C. 20001
(202) 879-3939
(202) 626-1700 (Fax)
gdnager@jonesday.com
bolcott@jonesday.com
rwatson@jonesday.com
vsuri@jonesday.com

Andrew D. Lipman
Russell M. Blau
David B. Salmons
Catherine Kuersten
MORGAN, LEWIS & BOCKIUS LLP
1111 Pennsylvania Ave, NW
Washington, DC 20004
(202) 739-3000
(202) 739-3001 (Fax)
andrew.lipman@morganlewis.com
russell.blau@morganlewis.com
david.salmons@morganlewis.com
catherine.kuersten@morganlewis.com

Counsel to Huawei Technologies Co., Ltd. and Huawei Technologies USA, Inc.

LIST OF EXHIBITS

Exhibit A	Declaration of John Suffolk
Exhibit B	Declaration of Donald A. Purdy, Jr.
Exhibit C	Declaration of Thomas Dowding
Exhibit D	Declaration of Ariel Ye
Exhibit E	Declaration of Jihong Chen and Jianwei Fang
Exhibit F	Declaration of Allan L. Shampine
Exhibit G	Declaration of Bryant Tow
Exhibit H	Declaration of Emily Hammond
Exhibit I	Huawei Cybersecurity White Paper June 2016
Exhibit J	Huawei Cybersecurity White Paper December 2014
Exhibit K	Huawei Cybersecurity White Paper October 2013
Exhibit L	Huawei Cybersecurity White Paper September 2012
Exhibit M	"Nokia Signing a Joint Venture Agreement with China Huaxin to Establish Nokia Shanghai Bell"
Exhibit N	"Nokia 2016 Corporate Social Responsibility Report of Shanghai Nokia Bell"
Exhibit O	Certification and Testing of Huawei Products