IN THE UNITED STATES COURT OF APPEALS
FOR THE FIFTH CIRCUIT

NO. 19-60896

HUAWEI TECHNOLOGIES USA, INCORPORATED, AND
HUAWEI TECHNOLOGIES COMPANY., LIMITED,
PETITIONERS,

V.

FEDERAL COMMUNICATIONS COMMISSION
AND UNITED STATES OF AMERICA,
RESPONDENTS.

ON PETITION FOR REVIEW OF AN ORDER OF THE
FEDERAL COMMUNICATIONS COMMISSION

BRIEF FOR RESPONDENTS

JOSEPH H. HUNT
ASSISTANT ATTORNEY GENERAL

SHARON SWINGLE
DENNIS FAN
CIVIL DIVISION, APPELLATE STAFF

UNITED STATES
DEPARTMENT OF JUSTICE
WASHINGTON, D.C. 20530

THOMAS M. JOHNSON, JR.
GENERAL COUNSEL

ASHLEY S. BOIZELLE
DEPUTY GENERAL COUNSEL

JACOB M. LEWIS
ASSOCIATE GENERAL COUNSEL

MATTHEW J. DUNNE
SCOTT M. NOVECK
COUNSEL

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554
(202) 418-1740

CERTIFICATE OF INTERESTED PERSONS
REQUIRED BY 5TH CIR. R. 28.2.1

No. 19-60896, *Huawei Technologies USA, Inc., and Huawei Technologies Co., Ltd. v. Federal Communications Commission and United States of America*

The undersigned counsel of record certifies that the following listed persons and entities as described in the fourth sentence of Circuit Rule 28.2.1 have an interest in the outcome of this case. These representations are made for the judges of this Court to evaluate possible disqualification or recusal.

Parties:
Huawei Technologies USA, Inc.
Huawei Technologies Coöperatief U.A. (Netherlands)
Huawei Investment & Holding Co., Ltd (China)

Counsel:
Glen D. Nager
Michael A. Carvin
Shay Dvoretzky
Karl R. Thompson
Parker A. Rider-Longmaid
JONES DAY
51 Louisiana Ave., N.W.
Washington, D.C. 20001-2113

Andrew D. Lipman
Russell M. Blau
David B. Salmons
MORGAN, LEWIS & BOCKIUS LLP
1111 Pennsylvania Ave., N.W.
Washington, D.C. 20004

Joseph H. Hunt
Sharon Swingle
Dennis Fan
UNITED STATES DEPARTMENT OF JUSTICE
Washington, D.C. 20530

Thomas M. Johnson, Jr.
Ashley S. Boizelle
Jacob M. Lewis
Matthew J. Dunne
Scott M. Noveck
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

June 1, 2020

s/ Matthew J. Dunne

Matthew J. Dunne
Counsel
Federal Communications Commission
Washington, D.C. 20554

STATEMENT ON ORAL ARGUMENT

Respondents believe that this case can be resolved on the briefs but stand ready to present oral argument if the Court would find it helpful.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

ADMINISTRATIVE DECISIONS

STATUTES

REGULATIONS

CONSTITUTIONAL PROVISIONS

OTHER AUTHORITIES

JURISDICTION

This case concerns a petition for review of the Federal Communications Commission order, *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs; Huawei Designation; ZTE Designation*, 34 FCC Rcd 11423 (2019) (JA__) ("*Order*"). The FCC released the *Order* on November 26, 2019, and published a summary in the Federal Register on January 3, 2020. 85 Fed. Reg. 230. Petitioners petitioned for review on December 4, 2019, and January 6, 2020. Petitioners invoke this Court's jurisdiction under 47 U.S.C. §402(a) and 28 U.S.C. §§2342 & 2344. However, as we explain below, the Court lacks jurisdiction over the entire petition because it is not ripe, and separately over the portion of the *Order* initially designating Huawei as a covered company because that is not "final action." *See* 28 U.S.C. §2342(1).

INTRODUCTION

Congress entrusted the FCC with the responsibility to act as a faithful steward of the Universal Service Fund ("USF")—a federal-subsidy program designed to provide telecommunications service providers with incentives to build out reliable, advanced communications networks (like high-speed broadband) throughout the country. To guide the Commission's discretion in allocating the Fund, Congress provided a non-exhaustive list of policy

objectives for the Commission to consider, including that "[q]uality services should be available at just, reasonable, and affordable rates," and that the provision of such services should be "consistent with the public interest, convenience, and necessity." 47 U.S.C. §§254(b), (c). This Court has recognized that these "guiding principles reflect congressional intent to delegate difficult policy choices to the Commission's discretion." *Alenco Commc'ns, Inc. v. FCC*, 201 F.3d 608, 615 (5th Cir. 2000).

In the *Order* under review, the Commission unanimously determined that it would be inconsistent with the "public interest," and deter the provision of "quality" services, to distribute USF funds for equipment or services from companies that threaten "the integrity of communications networks or the communications supply chain." *Order* ¶¶26, 29, 31 (JA__, __, __). The Commission reasonably concluded, based on an extensive record, that networks with security vulnerabilities that could permit foreign surveillance or service disruption were not "quality" networks capable of furthering the goal of universal service. *Order* ¶29 (JA__). "Where the statutory language does not explicitly command otherwise," this Court "defer[s] to the agency's reasonable judgment" about what ambiguous terms like "quality" mean in the Act. *Tex. Office of Pub. Util. Counsel v. FCC*, 183 F.3d 393, 437 (5th Cir. 1999) ("*TOPUC I*") .

Huawei challenges the FCC's decision to exclude carriers whose networks are vulnerable to foreign interference, contending that the FCC has neither statutory nor constitutional authority to make policy judgments involving "national security." These arguments are premature, as Huawei has not yet been injured by the *Order*. They are also meritless. The Commission has a "specific, but important" role to play here, *Order* ¶4 (JA__)—evaluating domestic communications networks and supply chains for security flaws. These technical issues are well within the Commission's core, Congressionally-delegated expertise, even though they may involve national security considerations.

Huawei's claim that the Communications Act textually commits all policy determinations with national security implications to the President is demonstrably false. Congress created the FCC in part "for the purpose of the national defense" and "promoting safety of life and property," 47 U.S.C. §151. The FCC may also refuse a radio license to a foreign-owned entity, *id.*, §310(b)(4), and deny certificates to foreign carriers seeking to operate in U.S. markets, *see id.* §214, if contrary to the public interest. With respect to the Constitution, Huawei nowhere explains, nor could it, how the Commission's consideration of network integrity in administering a federal subsidy program intrudes on the President's powers. In any event, the Court need not reach

that constitutional issue here, because other executive branch agencies and the FCC all concur in the appropriate policy outcome.

Huawei also challenges its initial designation as a company whose products and services should be excluded from the USF, but that challenge is plainly premature. Carriers may still use USF funding for Huawei products or services unless and until the Commission makes a final designation decision—at which point, Huawei can seek judicial review. In any event, the Commission considered ample evidence that Huawei posed a potential threat to America's communications networks, including information it received from members of Congress and Executive agencies with national security expertise. Contrary to Huawei's suggestion, the Commission's reasoned consideration of relevant information from other government actors does not amount to impermissible "pretext" for the *Order*.

For these reasons, Huawei's petition for review should be denied.

QUESTIONS PRESENTED

1. Whether Huawei's challenge to the Commission's rule is ripe.

2. Whether the FCC has authority to prohibit the use of federal Universal Service funds to purchase equipment or services from companies that the agency finds, consistent with determinations by Congress and other

components of the Executive Branch, pose a national security threat to the integrity of communications networks or the communications supply chain.

3. Whether the FCC's rule effecting that prohibition was reasonable.

4. Whether the FCC's initial designation of Huawei as a company covered by the rule—which does not restrict the use of Universal Service funds unless and until the agency after further proceedings issues a final designation—is final agency action subject to judicial review.

5. Whether, if the initial designation is reviewable, it was reasonable and supported by sufficient evidence to warrant a final designation proceeding.

STATUTES AND REGULATIONS

The relevant statutes and regulations appear in an appendix to this brief.

COUNTERSTATEMENT

A. The FCC's Universal Service Program

The Federal Communications Commission was established in part "to make available…to all the people of the United States…communication service with adequate facilities at reasonable charges." 47 U.S.C. §151. This concept—known as "universal service"—"has [long] been a fundamental goal of federal telecommunications." *Alenco*, 201 F.3d at 614.

In the Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 64, Congress directed the FCC to adopt a system of explicit subsidies to promote universal service. *See TOPUC I*, 183 F.3d at 406. To that end, the Commission makes payments from the federal Universal Service Fund (USF) to telecommunications carriers, subsidizing service for: (1) areas that are comparatively expensive to serve, (2) low-income consumers, (3) rural health care facilities, and (4) schools and libraries. *Order* ¶22 (JA__). The USF is financed through contributions from carriers, and ultimately United States consumers. *See TOPUC I*, 183 F.3d at 407.

Section 254 of the Act describes the Commission's authority to administer the USF program. 47 U.S.C. §254. Three provisions are particularly relevant here. First, subsection 254(b) directs the Commission to base its universal service policies on seven principles, including that "[q]uality services should be available at just, reasonable, and affordable rates." *Id.* §254(b).

Second, subsection 254(c) states that the Commission shall periodically redefine "universal service" and should consider "the extent to which such" services "are consistent with the public interest, convenience, and necessity." 47 U.S.C. §254(c)(1)(D). This emphasis on the public interest is echoed in Section 201 of the Act, which authorizes the FCC to "prescribe such rules

and regulations as may be necessary in the public interest to carry out the provisions of" the Act. *Id.* §201(b).

Third, subsection 254(e) states that carriers that receive Universal Service support "shall use that support only for the provision, maintenance, and upgrading of facilities and services for which the support is intended." 47 U.S.C. §254(e). This provision authorizes "the FCC to determine and specify precisely how USF funds may or must be used." *In re FCC 11-161*, 753 F.3d 1015, 1046 (10th Cir. 2014).

B. The FCC's Responsibility for Network Security

Congress established the FCC also "for the purpose of the national defense" and "promoting safety of life and property through the use of…communication" 47 U.S.C. §151. Consistent with this general mandate, several provisions of the Communications Act require the Commission to consider the potential impact on network security or the public interest of permitting foreign-owned or -controlled entities access to different components of American communications networks.

For example, Section 310 of the Act states that no broadcast or common carrier radio license shall be granted to a corporation with a certain threshold of foreign ownership "if the Commission finds that the public interest will be served by the refusal or revocation of such license." 47 U.S.C.

§310(b)(4). *See Moving Phones P'ship L.P. v. FCC*, 998 F.2d 1051, 1055 (D.C. Cir. 1993) (noting "national security policy underlying the statute."). In conducting that analysis, the FCC recognizes "that foreign participation in the U.S. telecommunications market may implicate significant national security or law enforcement issues uniquely within the expertise of the Executive Branch," and considers comments from other Executive Branch agencies. *Rules & Policies on Foreign Participation in the U.S. Telecommunications Mkt.*, 12 FCC Rcd 23891, 23919 ¶62 (1997).

Similarly, under Section 214 of the Act, no carrier may provide service until the Commission certifies that "public convenience and necessity require" it. 47 U.S.C. §214(a). In performing that analysis, the Commission has for decades "consider[ed] whether such an application raises national security, law enforcement, foreign policy, or trade policy concerns related to the applicant's reportable foreign ownership." *China Mobile International (USA) Inc.*, 34 FCC Rcd 3361, 3362 ¶2 (2019) ("*China Mobile*"); *see also Hawaiian Tel. Co. v. FCC*, 589 F.2d 647, 657 (D.C. Cir. 1978) (in its Section 214 analysis, "the FCC reviewed and found persuasive…considerations of national security and cost effectiveness"). In this analysis, the agency also seeks "the expertise of the relevant Executive Branch agencies" and "accord[s] deference to their expertise when they…identif[y] such a concern

in a particular application." *China Mobile* ¶2; *see, e.g.*, *id.* ¶¶5, 6, 14 (referring to advice of Departments of Homeland Security, State, and Justice in denying Section 214 application of Chinese telecommunications company); *see Order* ¶20 (JA__); *see also* 47 U.S.C. §214(b) (requiring notification of Secretaries of State and Defense, among others).

The FCC's attention to foreign threats in securing the nation's networks has involved close coordination with other federal agencies. *See generally Order* ¶19 (JA__). On April 4, 2020, the President issued *Executive Order on Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector*, Exec. Order No. 13913, 85 Fed. Reg. 19643 (Apr. 4, 2020), which establishes a committee composed of the Attorney General and the Secretaries of Defense and Homeland Security, advised by several other departments and agencies, "to assist the FCC in its public interest review of national security and law enforcement concerns that may be raised by foreign participation in the United States telecommunications services sector." *Id.* §§1 & 3. The FCC may refer any pending license application from foreign entities to the Committee for review and a recommendation on whether the applications should be approved. *Id.* §§9-10.

C. Growing Concern with Huawei and Other Potential Threats to the Security of the Nation's Telecommunications Network

Over the past decade, Congress and actors throughout the Executive Branch have stressed the importance of addressing foreign threats to the U.S. communications networks and supply chain.

1. HPSCI Report

In November 2011, the House Permanent Select Committee on Intelligence investigated "the counterintelligence and security threat posed by Chinese telecommunications companies" doing business in the United States. *See Order* ¶7 (JA__); 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* at iv (Oct. 8, 2012) ("*HPSCI Report*").[1] The bipartisan investigation centered on Huawei Technologies Company and ZTE, the two largest Chinese telecommunications equipment manufacturers. *Id.* The Committee emphasized the telecommunications sector's "critical role" "in the safety and security of our nation," its status as "a target of foreign intelligence services,"

[1] Available at https://republicans-intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf.

and "the potential security threat posed by Chinese telecommunications companies with potential ties to the Chinese government or military." *Id.* at iv-v. It found that "China has the means, opportunity, and motive to use telecommunications companies for malicious purposes." *Id.* at 2.

The Committee was particularly troubled by numerous connections between Huawei and the Chinese government. It cited evidence that the Chinese Communist Party ensures that "national champions" in "strategic sectors"—a status purportedly enjoyed by Huawei—"dominate through a combination of market protectionism, cheap loans, tax and subsidy programs, and diplomatic support in the case of offshore markets." *Id.* at 21. It also found that "the Chinese Communist Party maintains a Party Committee within the company, but [Huawei] failed to explain what that Committee does on behalf of the Party," and more generally that its failure to provide information "undermines the company's repeated assertions that it is not inappropriately influenced by the Chinese government." *Id.* at 22. Interviews with current and former Huawei USA employees "describe[d] a company that is managed almost completely by the Huawei parent company in China." *Id.* at 13.

Ultimately, the Committee recommended that U.S. government agencies and federal contractors "exclude ZTE or Huawei equipment in their

systems," and "strongly encouraged" private-sector entities "to consider the…security risks associated with" Huawei and "to seek out other vendors for their projects." *Id.* at vi.

2. Increased Concern with Network Security

The concern that Huawei or other foreign entities could compromise the nation's network security has grown since. In 2017, Congress passed, and the President signed into law, the National Defense Authorization Act for Fiscal Year 2018 (2018 NDAA), which, inter alia, barred the Department of Defense from using "[t]elecommunications equipment [or] services produced…[or] provided by Huawei Technologies Company or ZTE Corporation" for certain critical programs. *See* Pub. L. 115-91, 131 Stat. 1283, 1762, §656.

The National Defense Authorization Act for Fiscal Year 2019 (2019 NDAA) went further. *See* Pub. L. 115-232, 132 Stat. 1636. Section 889(b)(1) of that Act prohibits executive agencies from spending loan or grant funds on equipment or services that use "covered telecommunications equipment or services" as a substantial component. *See id.* at 1917, §889 (b)(1). The law defines "covered telecommunications equipment or services" to include

telecommunications equipment with certain capabilities produced by Huawei or any of its subsidiaries. *Id.* at 1918, §889(f)(3).[2]

A May 15, 2019 Executive Order found that "foreign adversaries are increasingly creating and exploiting vulnerabilities in information and communications technology and services…in order to commit malicious cyber-enabled actions, including economic and industrial espionage against the United States." *Executive Order on Securing the Information and Communications Technology and Services Supply Chain*, Exec. Order No. 13873, 84 Fed. Reg. 22689 (May 15, 2019); *see Order* ¶17 (JA___). The order declares a national emergency, and prohibits the acquisition or use of communications technology or services that the Secretary of Commerce finds, in consultation with the FCC and several other entities, (1) are designed or supplied by persons with a nexus to a "foreign adversary," and (2) pose an undue risk to U.S. telecommunications technology and infrastructure or the national security. E.O. 13873 §1.

[2] Huawei's challenge to the statute as an unconstitutional Bill of Attainder was dismissed. *See Huawei Techs. USA, Inc. v. United States*, 2020 WL 805257 (E.D. Tex., Feb. 18, 2020).

D. *NPRM*

In response to these growing concerns, the Commission sought comment on a proposal to prohibit the use of USF funds to purchase or obtain equipment or services from providers identified as posing a national security risk to communications networks or the supply chain. *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, 33 FCC Rcd 4058 (2018) ("*NPRM*") (JA__). The *NPRM* sought comment on whether and how to implement the proposed prohibition and how to identify the "covered companies" subject to the rule. *Id.* ¶¶13-14, 19-23, 33-34 (JA__-__, __-__, __-__).

E. *Order*

In the *Order* on review, the Commission adopted a rule, codified at 47 C.F.R. §54.9, that prohibits the use of USF funds to purchase equipment or services produced or provided by a "covered company," defined as a company designated by the Commission as posing a national security threat to the integrity of communications networks or the communications supply chain. *Order* ¶¶28-38 (JA__-__).

The Commission also established a process to designate companies covered under the rule, *id.* ¶¶39-42 (JA__-__). It then "initially designated" Huawei and ZTE as covered companies, initiating a further proceeding—still

ongoing—to decide whether to issue a "final designation" triggering the restrictions on use of USF funds. *Id.* ¶¶43-63 (JA__-__).

1. Prohibition on USF Funds for Payments to Covered Companies

a. Purpose

The FCC explained that it had a "specific, but important, role to play in securing the communications supply chain," and a duty "within the confines of its legal authority to address national security threats" by "securing our nation's critical telecommunications infrastructure." *Id.* ¶4 (JA__). The Department of Justice agreed, stating in comments that "[o]ur national defense will depend on the security" of our networks, and protecting these networks from threats is "a vital national security goal." Letter from William P. Barr, Attorney General, to Ajit Pai, Chairman, Federal Communications Commission at 1 (Nov. 13, 2019) (JA__).

b. Authority under Section 254

The FCC found it had authority to prohibit USF recipients from spending those funds on covered companies. First, the agency concluded that "providing a secure service is part of providing a *quality* service," one of the Universal Service principles in Section 254(b)(1). *Order* ¶29 (emphasis added) (JA__). Second, the agency concluded that "the *public interest* requires that the USF support only services that are not dependent on

equipment and services provided or produced by any company that poses a national security threat," consistent with Section 254(c)(1)(D). *Id.* ¶31 (emphasis added) (JA__).

Finally, the agency noted that Section 889 of the 2019 NDAA prohibits the expenditure of loan or grant funds by federal agencies on certain telecommunications equipment or services as "contrary to the security interests of the United States." *Order* ¶38 (JA__). Although USF funds are not federal grants or loans, the Commission found "that the goals underlying [Section 889] also support our decision." *Id.*

c. Authority under CALEA

As an alternative basis for its decision, the FCC found that its rule implements Section 105 of the Communications Assistance for Law Enforcement Act (CALEA). *Order* ¶35 (JA__) (citing Pub. L. 103–414, 108 Stat. 4279, 4283, §105 (Oct. 25, 1994), codified at 47 U.S.C. §1004). CALEA requires U.S. telecommunications providers to ensure that their facilities allow law enforcement to intercept communications under certain circumstances. 47 U.S.C. §1003(a). Section 105 of CALEA further requires that carriers "ensure that any interception of communications…within its switching premises can be activated only in accordance with a court order or other lawful authorization." *Id.* at §1004. The agency explained that

prohibition of USF funds for equipment from covered companies "directly implements Section 105 of CALEA by reducing the likelihood that [carriers] use USF funds to facilitate unauthorized surveillance." *Id.* ¶¶35-36 (JA__-__).

2. Process for Designating Covered Companies

The agency also established a process for determining which companies will be subject to the rule's prohibition. Under that process, the agency issues an "initial designation" announcing it has initially determined that a given company poses a national security threat to the integrity of communications networks or the supply chain, as well as the basis for that determination. *Order* ¶40 (JA__). The initially-designated company and other interested parties may then file comments in response. If a party opposes designation, the designation will take effect only if the agency, after reviewing the full record, issues a "final designation." *Id.*; *see* 47 C.F.R. §54.9(b)(2). The agency must make this finding within 120 days, and any appeal to the full Commission must be decided within another 120 days, subject to extension for good cause. *Id.*

In making its initial and final designations, the Commission stated that it "will base its determination on the totality of evidence." *Id.* ¶41 (JA__). The agency will consider determinations by Congress, the President, or other

executive agencies that an entity poses a national security threat and will "seek to harmonize its determinations" with those of other federal agencies and the Legislative branch. *Id.* It may also consider classified information, which will not be made public nor available to the affected company. *Id.* And if the Commission later finds that a covered company no longer poses a national security threat, it will "promptly…revers[e] its designation" of that company. *Id.* ¶42 (JA__).

3. Initial Designation of Huawei.

In the *Order*, the FCC initially designated two Chinese companies, Huawei and ZTE, as covered companies. *Order* ¶¶39-64 (JA__-__). The Commission explained that

> Huawei and ZTE pose a unique threat to the security of communications networks and the communications supply chain because of their size, their close ties to the Chinese government both as a function of Chinese law and as a matter of fact, the security flaws in their equipment, and the unique end-to-end nature of Huawei's service agreements that allow it key access to exploit for malicious purposes.

Id. ¶45 (JA__).

The Commission focused on these companies based on a "'substantial body of evidence' about the risks" from Huawei and ZTE. *Order* ¶44 (JA__). The agency cited the following:

- *Ties to the Chinese Government and Military*—The Commission identified numerous ties between Huawei and China's government and military. *Order* ¶¶48-51 (JA__-__). Among other things, Huawei's founder is believed to be a former director of a military organization associated with Chinese signals intelligence, *id.* ¶50 (JA__); "the Chinese government maintains an internal Communist Party Committee within Huawei that can influence the company's operations and decisions," *id.*; and Huawei "is treated as a state-owned enterprise" that receives "vast subsidies from the Chinese government," *id.* ¶51 (JA__).
- *Chinese National Intelligence Law*—The Commission noted that Chinese law "permit[s] the government, including state intelligence agencies, to demand that private communications sector entities cooperate with any governmental requests, which could involve revealing customer information, including network traffic information." *Order* ¶46 (JA__). China's National Intelligence Law requires all organizations and citizens to "provide support" to State intelligence work," and it allows Chinese intelligence agencies "to take control of an organization's facilities, including communications equipment." *Id.* The Commission found "[t]his broad

authority…particularly troublesome, given the Chinese government's involvement in computer intrusions and attacks as well as economic espionage." *Id*.

- *Reported Cybersecurity Flaws*— The Commission cited reports from cybersecurity firms describing numerous vulnerabilities in Huawei's equipment, *Order* ¶¶54-57 (JA__-__), including one study finding that "over half of the Huawei firmware images analyzed had at least one potential backdoor that could allow an attacker with knowledge of the firmware to log into the device," *id.* ¶54 (JA__).
- *Risk Assessments from U.S. Government Authorities and Allies*— The FCC cited "actions of other agencies and branches of the government, along with the increasing caution urged by our nation's intelligence officials." *Id.* ¶52 (JA__). In addition to the *HPSCI Report* and 2019 NDAA cited above, for example, the Department of Justice commented "that it is pursuing numerous criminal charges against Huawei for violations of federal law" and "strongly support[ing]" limiting reliance on its equipment. *Id.* And the Department of Commerce added Huawei to its list of entities believed to "pose a significant risk" to national security. *Id.* ¶48 (JA__).

- *Risk Assessments from Allies*—The Commission also "rel[ied] on similar assessments by other countries." *Id.* ¶53 (JA__). In 2019, the United Kingdom's Huawei Cyber Security Evaluation Centre Oversight Board described "significant software engineering and cyber security problems" and "risks associated with Huawei's engineering processes." *Id.* ¶55 & n.170 (JA__). The Board also lacked confidence in Huawei's capacity "to successfully complete the…transformation program that it has proposed" to address these defects. *Id.* And a panel of NATO cybersecurity experts wrote that China has a "notorious reputation for persistent industrial espionage, and in particular for the close collaboration between government and Chinese industry." *Id.* ¶44 (JA__); *see id.* ¶53 (JA__) (citing actions of other governments and private carriers).
- *Classified Information*—While the FCC found the "publicly available information in the record…sufficient to support these designations," the agency also "compiled and reviewed additional classified national security information that provides further support for [its]

determinations." *Id*. n.124 (JA__). This information was contained in classified Appendix E to the *Order*. *Id*.[3]

F. Developments after the *Order*

On February 3, 2020, in the ongoing designation proceeding, Huawei filed 176 pages of comments, with voluminous attachments, arguing against a final designation. These comments remain under consideration, and the Commission has not yet issued a final determination.

Separately, on March 12, 2020, the President signed into law the Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 16-124, 134 Stat. 158 ("Secure Networks Act"), which prohibits the use of any federal subsidy administered by the FCC on "any covered communications equipment or service." *Id.* §3(a). It directs the Commission to publish within a year a list of covered equipment and services that "pose[] an unacceptable risk to the national security of the United States or the security and safety of United States persons," and are capable of certain functions. *Id.* §2. The agency must base its determination "solely" on a set of defined criteria, including that it is a covered equipment or service under the 2019 NDAA, *id.*

[3] We plan to move to submit the classified material under seal for the Court's review.

§2(c), which includes Huawei.[4] The FCC is "not required to revisit" action "that in whole or in part implements" section 3(a), "to the extent such action is consistent with" that section. *Id.* §3(b). As of the filing of this brief, the FCC has issued Public Notices seeking comments on the Act, but has not begun a rulemaking to implement it.

SUMMARY OF ARGUMENT

I. Huawei's rule challenge is not ripe because any injury it might sustain, namely the exclusion of its equipment and services from the federal USF program, will not occur unless the Commission determines—following a separate and ongoing proceeding with additional notice and comment—that Huawei should be finally designated.

II.A. The FCC's broad discretion under Section 254 of the Act to administer the Universal Service program includes ample authority for its rule barring the use of USF funds to purchase or obtain equipment or services from a company that poses a national security threat to the integrity of the nation's communications networks or supply chain. Section 254(b) requires the Commission to support "quality services," which the agency reasonably interpreted to permit it to prohibit the use of USF funds on products or

[4] The full text appears in the statutory appendix.

services from companies that could compromise the nation's networks. *Order* ¶30 (JA__). Section 254(c)(1)(D) further requires the agency to establish universal service "consistent with the public interest, convenience, and necessity." 47 U.S.C. §254(c)(1)(D). It was reasonable for the Commission to consider network security as part of the public interest in administering the Universal Service Fund, particularly given that the FCC was established in part "for the purpose of the national defense" and to "promot[e] safety of life and property through the use of…communication." 47 U.S.C. §151. Finally, Section 254(e)'s requirement that carriers spend USF funds only for the "facilities and services for which the support is intended" authorizes the agency to direct how those funds are used. Huawei's contention that the Commission cannot withhold federal subsidies for equipment and services that the agency finds—and other branches of government agree—will make communications networks unsafe would undermine these statutory commands. It would also be inconsistent with the Commission's discretion to balance the Act's policies, unless the text explicitly prohibits it. *See TOPUC I*, 183 F.3d at 437; *Alenco*, 201 F.3d at 615.

II.B. The FCC's role under CALEA to prescribe rules that "prevent…interception or access without…authorization" provides further authority for the rule. *See* 47 U.S.C. §229(a) & (b)(1). The *Order* implements

CALEA "by reducing the likelihood that [carriers subject to CALEA] use USF funds to facilitate unauthorized surveillance." *Order* ¶¶35-36 (JA__).

II.C. The rule does not impermissibly intrude into the executive power of the President. First, any such objection is entirely theoretical here because the FCC and the rest of the executive branch have reached the same policy conclusions. Among other things, Executive Branch officials have repeatedly expressed concern about foreign threats to the nation's communications network, and the Attorney General "strongly support[ed]" the draft *Order*, "particularly the proposed designation of Huawei." *11/14/19 Letter* at 1 (JA__).

But in any event, Huawei does not explain specifically how the FCC's administration of the USF program intrudes on the powers of the President under Article II, nor can it establish that the *Order* would be unconstitutional in all applications, as it must in a facial challenge.

III.A. The agency's decision to prohibit the use of USF funds on equipment and services from companies that pose a national security threat to communication networks was also reasonable and well-supported. The record showed a shared and growing concern about the potential for foreign interference in communications networks, and a recognition that disruption to network operations could have devastating effects. The FCC acted

responsibly in ensuring that the nation's communications networks would not be compromised by companies whose equipment or services pose such a threat.

III.B. The rule is not impermissibly vague. Threat assessments often require evaluation of intangibles in light of the available evidence. Here, the FCC's initial determination outlined the factors the agency considers relevant, and Huawei has challenged their application in the final designation process. While there may be borderline cases that introduce ambiguities under the rule, the allegations here—that Huawei's close ties to the Chinese government and security flaws in its products create serious risk to network security—fall squarely within any plausible interpretation of a national security threat.

III.C. The *Order's* cost-benefit analysis was reasonable. Although not required to perform a formal cost-benefit analysis under the Act or the APA, the Commission carefully calculated the likely cost of prohibiting the use of USF funds for Huawei and ZTE equipment, and balanced it against the benefits of avoiding risks through the rule. Far from ignoring Huawei's arguments in balancing these costs and benefits, the agency acknowledged and rejected Huawei's arguments in favor of a different cost-benefit calculus.

III.D-E. The FCC provided sufficient notice that it might bar USF funds to purchase equipment or services from companies posing a national security threat to the nation's communications network, including the process by which it might do so. The *NPRM* devoted an entire section to the topic and made several proposals, including citing a suggestion that "the Commission establish criteria for a 'trusted vendor' using a 'totality-of-the-circumstances approach.'" *NPRM* n.37 (JA__). The *Order* also considered and rejected the many arguments that Huawei insists were ignored.

IV.A-B. The Commission's decision to initially designate Huawei as a covered company is not final agency action subject to judicial review. That decision is not the consummation of the agency's decisionmaking process and does not itself impose any restrictions on the use of USF funds to purchase Huawei's equipment or services. Instead, it initiates a further administrative process, and has no legal consequences unless and until the agency issues a final designation.

V.A For the same reason, Huawei cannot complain of a due process violation because the initial designation has not deprived it of any protected interest. In any case, Huawei has received all of the process it was due. By initially designating the company, the Commission provided Huawei with notice that the agency is considering whether to finally designate Huawei as a

covered company, and gave Huawei the opportunity to show it should not be designated.

V.B. The initial designation is not impermissibly retroactive. An initial designation does not impose any legal disability, and even a final designation under the rule is not impermissibly retroactive because it only governs the prospective disbursement of USF funds. The rule also does not seek to punish or remedy past wrongdoing, but rather uses past conduct to evaluate present and future risk.

V.C. The *Order* identified ample basis to initiate a comprehensive investigation into whether Huawei's equipment and services could be exploited by the Chinese government. The record reflects that Huawei has close ties to China's government and military, is financially beholden to the Chinese government and must cooperate with any governmental requests from Chinese intelligence agencies. Cybersecurity firms have documented significant security vulnerabilities in Huawei equipment that could be exploited to intercept communications or disrupt communications networks. The Commission's decision to issue an initial designation is also consistent with and supported by the actions of Congress, other Executive Branch agencies, and international allies.

V.D. In its last-ditch effort to invalidate the *Order*, Huawei alleges that the FCC adopted the *Order* only under Congressional pressure. The *Order* belies that contention, as does the apparent consensus among other Executive Branch actors that Huawei likely poses a national security risk. Moreover, it is entirely proper for an agency to consider concerns expressed by Congress and other federal actors in deciding whether to adopt a rule to address a pressing problem.

STANDARD OF REVIEW

"A court reviewing an agency's interpretation of its authority under the statute it administers must engage with the two-step framework established in *Chevron*." *Acosta v. Hensel Phelps Constr. Co.*, 909 F.3d 723, 730 (5th Cir. 2018) (citing *City of Arlington v. FCC*, 569 U.S. 290, 296 (2013)); *Alenco*, 201 F.3d at 619. The court first asks "whether Congress has directly spoken to the precise question at issue." *City of Arlington*, 569 U.S. at 296 (quoting *Chevron U.S.A. Inc. v. N.R.D.C.*, 467 U.S. 837, 842-43 (1984)). If the "statute is silent or ambiguous," the court asks if the agency's construction is "permissible." *Chevron*, 467 U.S. at 843. "If both criteria are met,…then *Chevron* requires a federal court to accept the agency's construction of the statute, even if the agency's reading differs from what the court believes is

the best statutory interpretation." *Acosta*, 909 F.3d at 730 (quotation marks and citations omitted).

Review under the Administrative Procedure Act is likewise "narrow and deferential, requiring only that the agency 'articulate a rational relationship between the facts found and the choice made." *Tex. Coal. of Cities v. FCC*, 324 F.3d 802, 811 (5th Cir. 2003). "The question is not whether we would have preferred another way…but whether the agency's decision was a reasonable one." *Tex. Office of Pub. Util. Counsel v. FCC*, 265 F.3d 313, 320 (5th Cir. 2001) (*TOPUC II*). And "where issues of the public interest are involved," "[j]udicial deference to agency judgments is near its zenith." *City of Dallas v. FCC*, 165 F.3d 341, 354 (5th Cir. 1999).

Courts review constitutional claims *de novo*. *TOPUC I*, 183 F.3d at 419 n.34.

ARGUMENT

I. HUAWEI'S PETITION IS NOT RIPE.

The ripeness inquiry, rooted in Article III, prevents courts "from entangling themselves in abstract disagreements over administrative policies," and protects "agencies from judicial interference until an administrative decision has been formalized and its effects felt in a concrete way by the challenging parties." *National Park Hospitality Ass'n v. Dep't of the Interior*, 538 U.S. 803, 807-08 (2003).

Huawei's potential injuries stem from the possible exclusion of its products from the federal USF program. But those injuries will not materialize unless the Commission issues a final designation of Huawei, in a separate ongoing proceeding with additional notice and comment. This Court should not review Huawei's challenges until it is certain Huawei will be injured, when the Court will benefit from that record. *See Texas v. United States*, 523 U.S. 296, 300 (1998) ("A claim is not ripe for adjudication if it rests upon contingent future events that may not occur as anticipated, or indeed may not occur at all.").

In the meantime, USF carriers can be reimbursed for Huawei equipment and services, and Huawei cannot show that it will have to adjust its conduct now in response to the *Order*. The mere possibility that third

parties may alter their business dealings with Huawei on account of the *Order* does not make Huawei's claims ripe. *Cf. Choice Inc. of Texas v. Greenstein*, 691 F.3d 710, 715 (5th Cir. 2012) (internal citations omitted) (increased risk of license suspension causing "heightened state of vigilance" insufficient to ripen pre-enforcement challenge to state licensing procedures). And "[t]he burden of participating in future administrative…proceedings does not constitute sufficient hardship to overcome the agency's challenge to ripeness." *AT&T Corp. v. FCC*, 349 F.3d 692, 702 (D.C. Cir. 2003); *see also Ohio Forestry Ass'n, Inc. v. Sierra Club*, 523 U.S. 726, 735 (1998); *National Park Hospitality Ass'n*, 538 U.S. at 811.[5]

[5] This is not the unusual case in which this Court has found a case ripe because an invalid process would "eliminate[] a procedural safeguard promised by Congress." *Texas v. United States*, 497 F.3d 491, 499 (5th Cir. 2007); *see also Del. Dep't of Natural Res. & Envtl. Control v. FERC*, 558 F.3d 575, 579 (D.C. Cir. 2009) (distinguishing *Texas* as a case where State claimed it "had been deprived of an alleged statutory procedural protection"). Huawei may raise any of its challenges in a potential future appeal before the Commission and this Court.

II. THE FCC HAS AUTHORITY TO PROHIBIT THE USE OF USF FUNDS FOR EQUIPMENT AND SERVICES FROM COMPANIES THAT POSE A THREAT TO THE SECURITY OF THE NATION'S COMMUNICATIONS NETWORKS.

A. The Communications Act Vests The Commission With Broad Authority To Oversee The Expenditure of USF Funds.

1. The Rule Promotes The Provision Of Quality USF Services.

Section 254 of the Act authorizes the FCC to administer the Universal Service program. Subsection (b) states that the Commission "shall base policies for the preservation and advancement of universal service" on certain general principles, 47 U.S.C. §254(b), the first of which is that "[q]uality services should be available at just, reasonable, and affordable rates," *id.* §254(b)(1).

In the *Order*, the FCC determined that barring the use of USF funds for products or services that could compromise the nation's networks will promote "quality services." *Order* ¶30 (JA__). As the agency explained, the nation's communications networks are "vulnerable to various forms of surveillance and attack that can lead to denial of service, and loss of integrity and confidentiality of network services." *Id.* ¶5 (JA__). The Commission therefore found it "critical to the provision of 'quality service' that USF funds

be spent on secure networks" in order to avoid those threats. *Id.* ¶29 (JA__). In short, "providing a secure service is part of providing a quality service." *Id.*

This was a reasonable conclusion. Section 254 does not define "quality services," thus delegating to the agency authority to determine how best to achieve that goal. *See Alenco*, 201 F.3d at 620 (according "substantial judicial deference" in challenge to "whether the Commission has sufficiently and explicitly supported universal service in an open, competitive market). The definition is also consistent with other FCC conclusions that "privacy and network security are among the factors that can affect the quality and reliability" of communications services. *2015 Broadband Progress Report*, 30 FCC Rcd 1375, 1438 ¶105 (2015); *see also, e.g.*, *Tech. Transitions*, 29 FCC Rcd 1433, 1523, App. B ¶19 (2014) (applicants for certain USF funding required to protect network from "cybersecurity threats and vulnerabilities"); *Amendments to Part 4 of the Commission's Rules Concerning Disruptions to Commc'ns*, 31 FCC Rcd 5817, 5899 ¶210 (2016) ("To the extent that covered broadband providers receive…[USF] funding, it is logical to require a certain level of assurance in behalf of the end users who fund it.").

Huawei argues that "quality service" refers only to the ability to transmit "data accurately, reliably, and quickly" (Br. 33). But while speed and reliability are aspects of a quality service, there is nothing in Section 254(b)

that suggests they are the sole indicia of "quality." And even if they were, a network vulnerable to cybersecurity breaches or compromise by foreign intelligence cannot function "reliably" or "accurately." Steps to prevent such vulnerabilities therefore fit comfortably within even Huawei's preferred reading of "quality services."

Huawei also argues (Br. 48) that the *Order* undermines the statutory principle of "affordable" rates. The FCC "enjoys broad discretion" when balancing principles under Section 254(b). *Rural Cellular Ass'n v. FCC*, 588 F.3d 1095, 1103 (D.C. Cir. 2009). It found that affordable services could be provided by suppliers who pose no risk to national security, and in any event, the Commission would be "shirking [its] responsibility to the American public if [it] were to ignore threats to our security posed by certain equipment manufacturers simply because that equipment was cheaper." *Order* ¶30 (JA__).

2. The Rule Advances The Public Interest

The Communications Act also tasks the FCC with securing the public interest in the performance of its duties. Section 254(c)(1)(D) requires the agency to define universal service in a manner "consistent with the public interest, convenience, and necessity." 47 U.S.C. §254(c)(1)(D). Likewise, Section 201 of the Act authorizes the FCC to "prescribe such rules and

regulations as may be necessary in the public interest to carry out" the Act. *Id*. §201(b).

Here, the Commission construed its public interest obligation to encompass considering foreign threats to the integrity of domestic communications networks in distributing federal subsidies. This interpretation was reasonable and warrants deference. Indeed, the Commission's charge to advance the public interest in regulating communications has long been held to vest it with capacious authority. "[T]he touchstone" of "public interest" in the Act "is as concrete as the complicated factors for judgment in such a field of delegated authority permit; it serves as a supple instrument for the exercise of discretion by the expert body which Congress has charged to carry out its legislative policy." *FCC v. Pottsville Broad. Co.*, 309 U.S. 134, 138 (1940). And "the Supreme Court has 'repeatedly emphasized that the Commission's judgment regarding how the public interest is best served is entitled to substantial judicial deference." *Anniston Broadcasting Co. v. FCC*, 668 F.2d 829, 832 (5th Cir. 1982). Courts have also recognized that serving the public interest may require the FCC to consider aspects of national security. *See generally Moving Phones*, 998 F.2d at 1055 (discussing "national security policy" underlying ban on foreign ownership in 47 U.S.C. §310(b), which directs the

FCC to consider public interest in deciding certain applications); *Hawaiian Tel. Co.*, 589 F.2d at 657 (upholding FCC public interest determination that included "considerations of national security"). Likewise here, prohibiting the use of USF funds to purchase equipment or services from companies that pose a national security threat to the Nation's communications networks promotes the public interest. *See Order* ¶31 (JA__) (citing 47 U.S.C. §254(c)(1)(D)).

Huawei argues that the term "public interest" must "take meaning from the purposes of the regulatory legislation." Br. 32 (quoting *NAACP v. Fed. Power Comm'n*, 425 U.S. 662, 669 (1976)). Precisely right. Here, the Commission was established in part "for the purpose of the national defense" and "for the purpose of promoting safety of life and property through the use of wire and radio communications." 47 U.S.C. §151. Therefore, the Act itself provides that national defense and public safety are among the "purposes of the regulatory legislation" (*NAACP*, 425 U.S. at 669) that the Commission must consider in evaluating whether subsidizing particular networks is

consistent with the "public interest."[6] To be sure, the powers of the Commission are not "unlimited," *National Broadcasting Co. v. United States*, 319 U.S. 190, 216 (1943) (*see* Br. 32), but within the field of communications, they are "comprehensive," *id.* at 217, and "expansive," *id.* at 219. The ability to administer the USF program to promote network security falls comfortably within the Commission's charge to promote the public interest by evaluating the "scope, character, and quality of services." Br. 35 (quoting *Nat'l Broad. Co.*, 319 U.S. at 216).

3. The Rule Specifies The Use "For Which The Support Is Intended"

Section 254(e) states that carriers who receive Universal Service support "shall use that support only" for the "facilities and services for which the support is intended." 47 U.S.C. §254(e). This language is a delegation

[6] Huawei argues (Br. 36) that the "prefatory language" in section 151 does not itself confer authority. But a "statement of congressional policy"—such as those in section 151—"can help delineate the contours of statutory authority,"—here, the grants of authority in sections 254 and 201 to secure the public interest. *Comcast Corp. v. FCC*, 600 F.3d 642, 654 (D.C. Cir. 2010). *See Order* ¶¶31, 33-34 (JA__, __); *Nat'l Rifle Ass'n of Am., Inc. v. Bureau of Alcohol, Tobacco, Firearms, & Explosives*, 700 F.3d 185, 198 (5th Cir. 2012) (upholding regulation against statutory challenge based in part on "context" provided by statutory preamble).

"for the FCC to determine and specify precisely how USF funds may or must be used," including the "flexibility" "to encourage the deployment of the types of facilities that will best achieve the principles set forth in section 254(b)." *In re FCC 11-161*, 753 F.3d at 1046; *see id.* ("[I]t seems highly unlikely that Congress would leave it to USF recipients to determine what 'the support is intended' for.").

Huawei argues that, contrary to Section 254(e), the FCC cannot specify how USF support is used if a rule involves assessing the risk to the nation's communications networks. Instead, it argues, the Commission is powerless to prevent carriers from spending those federal subsidies on products and services that the agency finds will make communications network less safe. That reading is unreasonable and would create a senseless gap in the Commission's authority to ensure that USF funds are used for specific intended purposes.

B. The Rule Is Also Supported By CALEA's Protections Against Unauthorized Interception Of Communications

The Communications Assistance for Law Enforcement Act (CALEA) provides another basis for the Commission's rule. Under Section 105 of CALEA, every telecommunications carrier must "ensure that any interception of communications…within its switching premises can be activated only in accordance with a court order or other lawful authorization." 47 U.S.C.

§1004. CALEA also authorizes the FCC to prescribe implementing rules, including provisions "to require appropriate authorization to activate interception of communications" and "to prevent any such interception or access without such authorization." 47 U.S.C. §229(a) & (b)(1).

As the *Order* explained, "allowing equipment from untrusted suppliers to be part of a network" could give those suppliers "the ability to illegally activate interceptions or other forms of surveillance," "whether through the insertion of malicious hardware or software implants, remote network access maintained by providers of managed services, or otherwise." *Order* ¶35 (JA__). The *Order*'s ban on the use of USF funds on covered companies thus "directly implements section 105 of CALEA by reducing the likelihood that [carriers subject to CALEA] use USF funds to facilitate unauthorized surveillance." *Id.* ¶¶35-36 (JA__-__).

Huawei argues that the agency did not provide notice that it might rely on CALEA. Br. 37. But the *NPRM* cited to CALEA, 47 U.S.C. §1004, when it asked whether there were other statutory provisions that affect USF recipients' obligations regarding network security, or other sources of legal authority on which the agency should rely. *NPRM* ¶36 & n.64 (JA__).

Huawei's substantive challenges to the Commission's reliance on CALEA (Br. 38-40) are no more compelling. Huawei first argues that

CALEA is inapposite because it requires providers to prevent unauthorized interceptions within their switching premises, while the *Order* applies to all equipment from covered companies, not just switching equipment. Br. 38. But the Commission explained why it was both safer and more administrable to ban all equipment from covered companies rather than attempting a more tailored, but administratively more burdensome, approach. *Order* ¶¶67-70 (JA__).

Huawei next contends that because CALEA facilitates lawful interceptions by federal and state governments, it gives "no license to make national security judgments involving foreign states." Br. 39. But while the statute creates a mechanism for *lawful* interception by U.S. government entities, carriers have a duty to prevent all *unlawful* interception without differentiation. The agency thus had authority to make rules preventing unlawful interception by any entity, including foreign entities.

Finally, Huawei argues that the rule, if not overbroad, is unduly narrow, because it applies only to USF recipients, while CALEA applies to all telecommunications carriers. Br. 40. But the FCC may act incrementally. "[A]gencies…need not deal in one fell swoop with the entire breadth of a novel development; instead, 'reform may take place one step at a time, addressing itself to the phase of the problem which seems most acute to the

[regulatory] mind.'" *National Ass'n of Broad. v. FCC*, 740 F.2d 1190, 1207 (D.C. Cir. 1984) (citation omitted). Thus, in a proceeding addressing oversight of USF funds, the agency was entitled to guard against the facilitation of CALEA violations in the use of USF funds, even if it also might have the power subsequently to adopt a broader rule applicable to all carriers.

C. The *Order* Does Not Impermissibly Intrude On The President's National Security Prerogatives.

Huawei argues that, as a statutory and constitutional matter, the FCC cannot—and only the President can—make determinations that touch on national security. But Huawei does not indicate who other than the FCC has authority to dictate the terms of USF funding. By Huawei's reasoning, the Executive Branch must accept the possibility that federal subsidies will support a national security threat, a result far less consistent with the President's responsibilities in the field of national security. None of Huawei's arguments provides a basis to invalidate the *Order*.

First, Huawei alleges (Br. 28-29) that Congress made a conscious decision in the Communications Act to provide for national security judgments to be made exclusively by the President. But that is demonstrably false. Congress created the FCC in part "for the purpose of the national defense" and "promoting safety of life and property," 47 U.S.C. §151, and as

we explain elsewhere, *see supra* pp. 37-38, the Commission's statutory purposes necessarily inform the "public interests" that the Commission is charged with protecting. *See, e.g.*, 47 U.S.C. §310(b)(4) (license applications of corporations with certain levels of foreign ownership may be rejected "if the Commission finds that the public interest will be served by [such] refusal or revocation"); *id.* §214(a) (empowering Commission to grant certificates authorizing access to U.S. telecommunications markets).[7] *See supra* pp. 7-8. Huawei's argument that this Court should draw a negative inference from the Act's provision for certain national security judgments to be made by the President (*see* 47 U.S.C. §§305(c), 606(c), 606(d)) is therefore mistaken, and

[7] Congress has authorized the Commission to examine national security under other statutes as well. *See* 47 U.S.C. §1507 (in certain spectrum allocation, FCC shall consider "the future needs of homeland security [and] national security, and other spectrum users"); *id* §1008 (FCC to consider "effect on public safety and national security" in determining if CALEA compliance is achievable).

cannot provide a basis to prevent the Commission from considering network integrity here.[8]

Huawei's constitutional argument that "conferring national security authority on the FCC" would "raise serious separation-of-powers concerns" and "impede the President's ability to perform his constitutional duty" in the realm of national security, *Morrison* v. *Olson*, 487 U.S. 654, 691 (1988) (Br. 26-32) fares no better. The argument makes little sense on its own terms. Requiring independent agencies to *ignore* national security considerations is far more intrusive and inconsistent with the President's responsibilities to protect national security. If the FCC must take actions *regardless* of how those actions harmed the national security, or ignore foreign threats to account only for domestic ones, that result would itself undermine the President's Article II responsibilities. Nor is this arrangement unusual: Congress has granted authority to independent agencies to make judgments

[8] Huawei similarly errs in asserting, without support, that the FCC lacks expertise to make judgments bearing on national security. Br. 30-31. To the contrary, in administering Sections 214, 310, and other provisions of the Act, the Commission and its career staff in the Public Safety and International Bureaus, among others, routinely evaluate evidence (including classified intelligence) that bears on risks associated with foreign access to U.S. communications networks. The Commission also participates in inter-agency working groups relating to foreign threats to communications systems, such as the Information and Communications Technology Supply Chain Risk Management Task Force hosted by the Department of Homeland Security.

that fall within the agencies' core areas of expertise and include some consideration of national security concerns. For example, the Nuclear Regulatory Commission's "prime area of concern in the licensing context" is "national security, public health, and safety." *Vermont Yankee Nuclear Power Corp. v. NRDC*, 435 U.S. 519, 550 (1978).[9]

In any event, this case presents no opportunity for Huawei to obtain judicial relief based on a conflict with the President's prerogatives. The FCC's actions are completely consistent with the view of other executive agencies and the President, who all agree as to the appropriate policy outcome. The President and other Executive Branch agencies have repeatedly expressed their concerns about foreign threats to the nation's communications networks, and about the potential for disruption posed by Huawei in particular. The President signed the 2019 NDAA, which bans the use of federal grants and loans on Huawei equipment, *see* 2019 NDAA §889(b)(1) & (f)(3), as well as (more recently) the Secure Networks Act of 2019, which directs the FCC to issue rules forbidding the use of funds like the USF on covered equipment, including equipment from companies covered by the

[9] *See also, e.g.*, 15 U.S.C. §78dd(a) (authorizing SEC to prohibit transactions on foreign securities exchanges if in the "public interest"); 52 U.S.C. §30121 (prohibiting certain activity by foreign nationals in U.S. elections, in Act administered by FEC).

2019 NDAA. *See* Secure Networks Act §2 & (3)(c). *See also supra* p. 13 (E.O. 13873 declares a national emergency regarding "foreign adversaries…exploiting vulnerabilities in…communications technology"). And the Attorney General "strongly support[ed]" the draft *Order*, "particularly the proposed designation of Huawei and ZTE as covered companies for purposes of that rule." *11/14/19 Letter* at 1 (JA__).

Relatedly, Huawei mounts a facial challenge to the Commission's authority under the Act, which can only succeed if Huawei shows the *Order* would be unconstitutional in all its applications. *See, e.g.*, *Noatex Corp. v. King Constr. of Houston, L.L.C.*, 732 F.3d 479, 484 (5th Cir. 2013) (citing *United States v. Salerno*, 481 U.S. 739, 745 (1987)). Huawei does not attempt to make, nor could it make, such a demanding showing here. The Commission could in theory under Section 254 prohibit USF funds from flowing to carriers with insecure or vulnerable networks in a manner that would require no national security determinations—say, based entirely on a technical analysis that domestic component parts had vulnerabilities. And an as-applied challenge fares no better where the FCC's actions are consistent with those taken by Congress and the President, regarding Huawei, eliminating any possible constitutional issue in its own case.

Even supposing the remote possibility that the FCC's national security judgments could depart from those of the President in some future case, no constitutional issue would be presented so long as the Commission abided by an established process—developed and approved by the President and other executive branch actors—for the FCC to reach those judgments. Historically, and now formally under an Executive Order, other executive agencies have advised the FCC on national security and law enforcement issues. *See* E.O. 13913. The Commission has "sought the expertise of the relevant Executive Branch agencies for over 20 years, and has accorded deference to their expertise when they have identified such a concern in a particular application." *China Mobile* ¶2. That other executive agencies facilitate the FCC's national security determinations, and that the FCC affords appropriate weight to those agencies' views when provided, only confirms that there are no apparent "risks to the effective functioning of government" here that warrant vacating the *Order* based on Article II concerns. *Nixon v. Fitzgerald*, 457 U.S. 731, 751 (1982). Instead, risks to the President's ability to protect the national security would only increase if this Court were to vacate the *Order*.

Finally, any constitutional doubts about the FCC's authority are not sufficiently serious to overcome the FCC's reasonable construction of its

authorities. *See Reno v. Flores*, 507 U.S. 292, 314 n.9 (1993). This Court's case law thus requires deference to the FCC's construction of Section 254 "[w]here the statutory language does not *explicitly command* otherwise." *TOPUC I*, 183 F.3d at 437 (emphasis added). Even if national security is not expressly mentioned in connection with the Section 254 public interest determination, this Court has recognized that so long as the Commission does not violate an express statutory command, it may use the universal-service mechanism to achieve policy objectives contained elsewhere in the Act. *See id.* (construction of "sufficient" level of service used to further Act's competition goals); *Alenco*, 201 F.3d at 615 (similar). So, too, here, where the Commission has exercised its public-interest authority to ensure that USF funds will be spent consistent with the national defense and public safety.[10]

[10] Huawei's suggestion that the six enumerated criteria in Section 254 are the "exclusive" policy goals the Commission may consider in administering the USF funds (Br. 27-28) thus conflicts with this Court's prior decisions. Also, as the *Order* explains, the Commission has the authority to determine what constitutes "universal service" on an ongoing basis, and may decide itself that the appropriate level of service requires protection from national security threats, whether or not based on a recommendation from the Federal-State Joint Board on Universal Service. *See Order* ¶ 32 (citing 47 U.S.C. §254(c)(1)).

III. THE PROHIBITION ON THE USE OF USF FUNDS TO OBTAIN EQUIPMENT OR SERVICES FROM COVERED COMPANIES WAS REASONABLE.

A. The Security Of The Nation's Communications Networks Is Critical And At Risk.

The record below illustrated both that "[m]odern communications networks are an integral component of the U.S. economy" and that "these networks are vulnerable to various forms of surveillance and attack that can lead to denial of service, and loss of integrity and confidentiality of network services." *Order* ¶5 (JA__).

A 2013 Presidential Policy Directive, for example, directed federal agencies to identify vulnerabilities in communications infrastructure and "to increase the security and resilience of critical infrastructure within the communications sector." *Order* ¶8 (JA__). A GAO report the same year identified means that "[a] potential enemy" might use to "exploit vulnerabilities in the communications equipment supply chain, such as placing malicious code in the components that could compromise the security and resilience of the networks." *Id.* ¶9 (JA__).

The agency considered the 2018 and 2019 NDAAs, which forbid certain purchases from companies deemed a threat to network security, *id.* ¶¶12-13. It also considered the *HSPCI* report, *id.* ¶7 (JA__), which found that the nation's network was "a target of foreign intelligence services," and

"highlighted the potential security threat posed by Chinese telecommunications companies with potential ties to the Chinese government or military." *HSPCI Report* at iv-v. The FCC also took note of Executive Order 13873, which declared a national emergency due to "foreign adversaries…increasingly creating and exploiting vulnerabilities in information and communications technology and services" to commit cybercrimes, "including economic and industrial espionage against the United States." E.O. 13873; *see Order* ¶¶12-17 (JA__-__); *supra* pp. 12-13. Given this record, the Commission reasonably determined that foreign-owned or -controlled companies could threaten domestic communications networks, and that USF subsidies should not flow to such companies.

B. The Rule Is Not Impermissibly Vague.

Huawei argues that the rule violates the APA and due process because, in defining a covered company as an entity "posing a national security threat to the integrity of communications networks or the communications supply chain," *Order* App. A, 47 C.F.R. §54.9(b) (JA__), the rule is "vague and standardless." Br. 51-57. Not so.

Where, as here, a law "'implicates no constitutionally protected conduct'" such as free speech, a court "should uphold [a vagueness] challenge only if the enactment is impermissibly vague in all of its

applications." *Roark & Hardee LP v. City of Austin*, 522 F.3d 533, 548 (5th Cir. 2008) (quoting *Village of Hoffman Estates v. Flipside, Hoffman Estates, Inc.*, 455 U.S. 489, 494-95 (1982)); *see Home Depot, Inc. v. Guste*, 773 F.2d 616, 628 (5th Cir. 1985) ("economic regulation is subject to a less strict vagueness test").

While the *Order* does not define all of the circumstances that may constitute a "national security threat," regulatory criteria are not vague "simply because they fail to delineate a set of factors relevant to a threat assessment." *Kashem v. Barr*, 941 F.3d 358, 372 (9th Cir. 2019). "Nor are the criteria vague merely because they fail to specify the "degree of risk inherent in the concept of a 'threat.'" *Id.* "Many perfectly constitutional statutes use imprecise terms like 'serious potential risk' ... or 'substantial risk' ...." *Id.* (citing *Sessions v. Dimaya*, 138 S. Ct. 1204, 1214 (2018)). Indeed, it is often infeasible to specify in advance all of the factors that may be salient when assessing a national security threat to the communications network or supply chain. *Cf. Schall v. Martin*, 467 U.S. 253, 279 (1984) ("a prediction of future criminal conduct is 'an experienced prediction based on a host of variables' which cannot be readily codified").

Moreover, while it may be challenging to define terms like "national security" in the abstract, an agency may "flesh out its rules through

adjudications and advisory opinions." *Council for Urological Interests v. Burwell*, 790 F.3d 212, 226 (D.C. Cir. 2015). In this case, the initial designation makes clear to the company in question what factors are relevant in a particular case, and the company has a full opportunity before any final designation to argue that those factors do not amount to a national security threat.

Finally, even if some theoretical case might raise questions about the precise contours of the term "national security threat," this case does not—the *Order* addresses alleged security flaws in Huawei equipment and the company's ties to the Chinese Government that could allow the interception of communications or the disruption of the U.S. communications network. The agency cited, for example, "Huawei's established relationship with the Chinese government as well as Huawei's obligation under Chinese law to cooperate with requests by the Chinese government for access to their system," *Order* ¶48 (JA__), evidence of a "'high number' of security vulnerabilities" in Huawei equipment, *id.* ¶54 (JA__), and evidence that that the "Chinese government has the 'means, opportunity, and motive to use telecommunications companies for malicious purposes,'" *id.* ¶58 (JA__). *See* Part IV.C (detailing allegations and support). Those allegations fall squarely within any possible definition of a "national security threat to the integrity of

communications networks or the communications supply chain" and were sufficient to merit further inquiry.

A "'plaintiff who engages in some conduct that is clearly proscribed cannot complain of the vagueness of the law as applied to the conduct of others.'" *Roark & Hardee*, 522 F.3d at 548 (quoting *Village of Hoffman Estates*, 455 U.S. at 494-95). In a recent case, for example, a person who had traveled to Somalia to "fight for Jihad and train for Jihad" challenged as unconstitutionally vague the criteria for the government's No-Fly list, which covered persons reasonably suspected of engaging in "terrorism and terrorist activities." *See Kashem*, 941 F.3d at 365, 373. The court rejected the challenge, stating, "[t]his case does not require us to address whether further precision was required in the abstract. Even if the criteria might be vague as applied to others…this is an as-applied challenge, and we are persuaded that each of *these plaintiffs* had fair notice that *his conduct* would raise suspicion under the criteria." *Id.* Huawei is in the same position here.

C. The Commission Reasonably Balanced The Costs And Benefits Of The Rule.

In adopting the rule, the Commission reasonably concluded that "the benefits…to the American economy, commerce, and consumers are likely to significantly and substantially outweigh the costs by a large margin." *Order* ¶109 (JA__).

In evaluating costs, the FCC considered the anticipated rate of equipment replacement by carriers, replacement costs, and effects on competition if use of Huawei and ZTE equipment and services was no longer subsidized, *Order* ¶¶110-120 (JA__-__), calculating an upper bound of $960 million, *see id.* (costs likely to be "much lower").

On the other side of the ledger, the FCC opined that the benefits of the rule included avoiding network disruption and surveillance, as well as possible data breaches, *Order* ¶109 (JA__), and that these benefits, while difficult to quantify, are likely to be substantial. The agency noted that "the digital economy accounted for $1.35 trillion of our economy in 2017, and so preventing a disruption of even 0.072% [of that value] would mean the benefits of the rule outweigh the costs." *Id*. The Commission found it "likely that any potential disruption would far exceed" that measure "given "how dependent…the digital economy…is on our national communications network and how interconnected that network is and is becoming." *Id.* The Commission further reasoned that if the rule reduced "malicious cyber activity" or "data breaches on consumers," by even a small percentage, the benefits of the rule would also "substantially outweigh the costs by a large margin." *Id*.

Finally, the Commission acknowledged additional qualitative benefits, including "preventing untrustworthy elements in the communications network from impacting our nation's defense, public safety, and homeland security operations, our military readiness, and our critical infrastructure," as well as "the collateral damage such as loss of life that may occur with any mass disruption to our nation's communications networks." *Id.*

Huawei argues that the rule threatens to forego the price and quality benefits that flow from Huawei's "presence in the marketplace." Br. 48. The FCC reasonably rejected this contention on the ground that many companies were "provid[ing] quality services at reasonable and affordable rates using suppliers" that did not raise quality or national security concerns. *Id.* ¶30 (JA__). The FCC further explained that Huawei's low rates appeared to result from subsidies from the Chinese government, and the agency predicted that eliminating subsidized companies from the market "should unleash competition from more-trusted, higher-quality suppliers in the long run, resulting in significant public interest benefits." *Id.* In any event, the agency stated, "we would be shirking our responsibility to the American public if we were to ignore threats to our security posed by certain equipment manufacturers simply because that equipment was cheaper." *Id.* ¶30 (JA__).

Huawei also argues it was irrational to calculate the costs of the rule based only on its potential application to Huawei and ZTE because other carriers may later be designated. Br. 48. But the Commission reasonably worked with the information it had. Huawei and ZTE are the only companies that were initially designated, and the Commission had no basis on which to estimate the costs of applying the rule to an unspecified number of companies with unspecified characteristics.

Huawei next argues that the Commission's analysis was irrational because the agency assumed that the rule would prevent some level of service disruption. Br 50-51. But the rule is designed to eliminate the use by USF recipients of equipment and services from companies that pose a national security threat, and it was reasonable for the Commission to suppose that excluding such companies would help secure the communications network against disruption. As the Commission explained, given the importance of network communications to the economy, even a small increase in security would have overwhelming benefits. *Order* ¶109 (JA__).

Finally, Huawei argues it was unreasonable to reject a "risk-based approach," and to instead "blacklist[]" whole companies. Br. 51. But the agency explained that, in its judgment, a complete ban on USF funds flowing to designated companies was the "only reliable protection against potential

incursions." *Order* ¶67 (JA__); *see id* ¶68 (JA__) (finding that vulnerabilities can be built into communications equipment beyond "the…company's flagship equipment," and the agency was unwilling to "allow for bad actors to circumvent our prohibitions through clever engineering."). A company-wide ban would also provide "regulatory certainty and…be easier for providers to implement and for the Commission to enforce," reducing compliance costs. *Id.* ¶69 (JA__).

D. The Commission Provided Sufficient Notice Of The Designation Process.

Huawei argues that the *NPRM* provided insufficient notice of the agency's designation process. Br. 40-43. But the *NPRM* had an entire section devoted to the topic. *See NPRM* ¶¶19-23 (JA__).

The Commission sought "comment broadly on possible approaches to defining the universe of companies covered by our proposed rules," and offered several different proposals. *Id.* One proposal was "for the Commission to establish the criteria for identifying a covered company" and asked how the Commission should determine those criteria. *Id.* ¶20 (JA__). In another proposal, the agency sought comment on relying on the 2018 and 2019 NDAAs, which specifically mention Huawei. *Id.* The *NPRM* also cited a suggestion that "the Commission establish criteria for a 'trusted vendor' using a 'totality-of-the-circumstances approach.'" *Id.* n.37 (JA__).

The APA requires an agency to provide notice of "either the terms or substance of the proposed rule or a description of the subjects and issues involved." 5 U.S.C. §553(b)(3). A proposal must "fairly apprise[] interested persons of the subjects and issues the agency is considering." *Chem. Mfrs. Ass'n v. EPA*, 870 F.2d 177, 203 (5th Cir. 1989). By highlighting the designation process and offering proposals, the *NPRM* provided sufficient notice under the APA. 5 U.S.C. §553(b)(3).

Huawei suggests that the Commission's notice was insufficient because the proposals for the designation process in the *NPRM* differed from those adopted in the *Order*—for example the final rules use separate initial and final designations, written comments, and delegate some authority to the Public Safety Bureau. Br. 43. But a "notice need not specifically identify every precise proposal which the agency may ultimately adopt as a final rule." *Chem. Mfrs. Ass'n*, 870 F.2d at 203 (citation and quotation marks omitted); *see Agape Church, Inc. v. FCC*, 738 F.3d 397, 412 (D.C. Cir. 2013) (final rules need not be "coterminous" with original proposals). Rather, "a new comment period will not be required so long as the modified rule is a logical outgrowth of the published proceedings." *TOPUC II*, 265 F.3d at 326 (quotation marks and citations omitted). Here, the agency clearly "apprise[d] interested persons of the subjects and issues [it was] considering" in the

initial *NPRM*, *Chem. Mfrs. Ass'n*, 870 F.2d at 203, by seeking comment on proposals for identifying covered companies, including considering the "totality-of-the-circumstances." *Order* n.37 (JA__).

E. The Commission Reasonably Considered And Rejected Huawei's Other Arguments

The FCC considered and rejected the factual contentions and legal arguments that Huawei says the agency "ignored," "largely disregarded," or failed to "meaningfully consider." Br. 45-47. The Commission considered the potential impact of its rule on the cost and availability of networking equipment for rural carriers and customers (Br. 45-46) and found that the benefits of network security outweighed those costs, *see Order* ¶67 (JA__) (citing Huawei comments). It also found that the record established service could be provided at affordable rates without Huawei and ZTE. *Id* ¶30 (JA__). It considered arguments that the rule failed to address other suppliers with operations in or components from China (Br. 46), and explained that Huawei and ZTE present a "unique" risk because of their size, ties to the Chinese government, security flaws, and end-to-end service model. *Order* ¶45 (JA__). It considered arguments that it should ban only switching equipment (Br. 46), and explained why it was both safer and more administrable to target all equipment from a covered company. *Order* ¶¶66-69 (JA__-__).

The agency also rejected legal arguments (Br. 47) that it lacked expertise or authority to make judgments implicating national security based both on the Communications Act and its "long history of considering national security equities." *Order* ¶¶33-34 (JA__-__) (citing Huawei comments). *See supra* pp. 12-13. And it rejected arguments (Br. 47) that Chinese law is purportedly irrelevant to U.S.-based subsidiaries of Chinese companies, noting that the Chinese government can exert influence over all elements of Chinese companies. *Order* ¶49 & nn.146-47 (JA__) (citing Huawei comments).

Finally, Huawei notes its contention that the rule was invalid under the Appointments Clause and *Lucia v. SEC*, 138 S. Ct. 2044, 2051-55 (2018) because the *Order* delegated authority to the Chief of the Public Safety and Homeland Security Bureau. Br. 47 (citing 11/14/2019 comments at 19 (JA__)). Huawei made this passing reference in a single sentence, buried in a list of "additional reasons" that the rule was purportedly invalid. "The Commission need not sift pleadings and documents to identify arguments that are not stated with clarity by a petitioner." *Bartholdi Cable Co., Inc. v. FCC*, 114 F.3d 274, 279 (D.C.Cir.1997) (internal quotation marks and citation omitted); *see TOPUC II*, 265 F.3d at 329 n.7 (agency "only has to address significant comments"). In any case, the argument is meritless. Putting aside

whether an FCC Bureau Chief is an "Officer of the United States" within the meaning of the Appointments Clause, U.S. Const. art. II, §2, cl. 2, under internal Commission procedures, FCC Bureau Chiefs are appointed by the full Commission, unlike the ALJs in *Lucia*, 138 S. Ct. at 2050.

IV. THE INITIAL DESIGNATION IS NOT FINAL AGENCY ACTION SUBJECT TO JUDICIAL REVIEW

A. The Initial Designation Merely Initiates An Adjudication And Has No Present Legal Consequences.

Apart from the reasons why the entire petition is unripe, Huawei's challenge to its initial designation also fails because that action is not final. Congress has provided for judicial review only of "final order[s]" of the FCC. 28 U.S.C. §§2342(1), 2344. That language incorporates the APA's "final agency action" requirement. *U.S. West Commc'ns, Inc. v. Hamilton*, 224 F.3d 1049, 1054-55 (9th Cir. 2004); *cf. Luminant Generation Co. v. U.S. EPA*, 757 F.3d 439, 441 (5th Cir. 2014) ("final action" under the Clean Air Act has the same meaning as "final agency action" under the APA). Huawei's initial designation therefore is reviewable only if it constitutes "final agency action for which there is no other adequate remedy in a court." 5 U.S.C. §704.

Agency action is final under this standard only when two conditions are satisfied. "First, the action must mark the consummation of the agency's decisionmaking process—it must not be of a tentative or merely interlocutory

nature." *Bennett v. Spear*, 520 U.S. 154, 177-78 (1997) (citation and internal quotation marks omitted). "[S]econd, the action must be one by which rights or obligations have been determined or from which legal consequences will flow." *Id.* at 178 (citations and quotation marks omitted). And even then, review is available only if the party seeking review has no other adequate means to obtain judicial relief. *Louisiana State v. U.S. Army Corps of Eng'rs*, 834 F.3d 574, 580-81 (5th Cir. 2016) (citing *Sackett v. EPA*, 566 U.S. 120, 127 (2012)).

The *Order*'s initial designation does not satisfy either prong. First, an initial designation is not the consummation of the Commission's decisionmaking process, but instead merely initiates further proceedings to determine whether a final designation is justified. At most, the initial designation represents a tentative view or an interlocutory step pending further process and a full opportunity for public comment. That is not final agency action. *See Luminant*, 757 F.3d at 442 (EPA notice of violation "does not end the [agency's] decisionmaking" because it "does not commit the [agency] to any particular course of action" and the agency "could choose to withdraw or amend the notice or take no further action").

Second, the initial designation does not, standing alone, have any legal consequences or affect any of Huawei's rights or obligations. The initial

designation does not trigger any restrictions on the use of USF funds to purchase Huawei's equipment or services; those consequences would flow only from a final designation. *See Order* ¶¶169-70 (JA___-__); 47 C.F.R. §54.9(b)(2) (JA___) ("If any party opposes the initial designation, the designation shall take effect only if the [agency]…issue[s] a second public notice announcing its final designation…."). Thus, the initial designation is merely an "intermediate decision [that] has no legal force," because "[f]urther proceedings are required before [the agency] can issue an order which has conclusive legal consequences." *Am. Airlines v. Herman*, 176 F.3d 283, 292 (5th Cir. 1999) (internal quotation marks omitted). Nor does the initial designation "bind[] the agency" in any way or "retract [the] agency's discretion to adopt a different view" when it reviews the full record to decide whether to issue a final designation. *Texas v. EEOC*, 933 F.3d 433, 441-42 (5th Cir. 2019).

The initial designation here is akin to the administrative complaint that the Supreme Court held was non-final in *FTC v. Standard Oil Co. of California*, 449 U.S. 232 (1980). There, the FTC issued a complaint averring that it "had reason to believe" that several companies were engaged in unfair methods of competition or deceptive acts or practices. *Id.* at 234. That complaint initiated further "adjudicatory proceedings" that could culminate in

an order to cease and desist the challenged practices. *Id.* at 241. Though the complaint accused the companies of wrongdoing and subjected them to the expense and disruption of defending themselves, the Court held that it was not final agency action subject to judicial review because the complaint "itself [was] a determination only that adjudicatory proceedings will commence," *id.* at 241-42, and had "no legal force or practical effect…other than the disruptions that accompany any major litigation," *id.* at 243. Moreover allowing interlocutory review of the complaint could "lead to piecemeal review" and "den[y] the agency an opportunity to correct its own mistakes and to apply its expertise." *Id.* at 242.

Though Huawei contends that carriers may be more hesitant to do business with it after the initial designation, "any such consequences are practical, as opposed to legal, ones." *Louisiana State*, 834 F.3d at 583. These "adverse economic effects" are simply "pragmatic[]" consequences that "accompany many forms of indisputably non-final government action," not legal consequences that stem from a change in legal status. *Air Brake Sys., Inc. v. Mineta*, 357 F.3d 632, 645 (6th Cir. 2004) (Sutton, J.). Thus, even if "[i]nitiating an enforcement proceeding against a company…may have a devastating effect on the company's business," that indirect economic

consequence "does not make the agency's action final." *Id.* (citing *Standard Oil* and other cases).

B. Huawei's Substantive Challenges To Its Designation Are A Matter For The Agency In The Ongoing Administrative Proceeding.

In the ongoing administrative proceeding before the FCC, Huawei has presented extensive argument and evidence to the Commission on whether to issue a final designation. In response to the initial designation, Huawei filed a 176-page principal submission, with 4,845 pages of supporting exhibits.[11] The matter is currently before the agency.

If Huawei remains dissatisfied after the Commission issues a final determination, it can seek judicial review and renew any arguments at that time. But Huawei's opportunity to seek judicial review, on a fully developed record and with a definitive determination from the agency, forecloses its attempt to engage in premature adjudication of its challenges now.

---

[11] *See* https://www.fcc.gov/ecfs/search/filings?proceedings_name=19-351&q=filers.name:(*Huawei*)&date_received=%5Bgte%5D1900-01-01%5Blte%5D2020-02-03. Huawei repeatedly cites those later-submitted comments here (*e.g.*, Br. 46-47, 74-78), which further illustrates that the initial designation is not final. In any case, a court may not review FCC action based on evidence or arguments "upon which the Commission…[was] afforded no opportunity to pass." 47 U.S.C. §405(a).

* * *

Because the initial designation is not final agency action, Huawei may not prematurely seek judicial review of the initial designation "[as] a means of turning prosecutor into defendant before adjudication concludes." *Standard Oil*, 449 U.S. at 243. That is so even when a party argues that the agency lacks statutory authority to conduct the proceeding at all. *Veldhoen v. U.S. Coast Guard*, 35 F.3d 222, 225 (5th Cir. 1994) (citing *Aluminum Co. of Am. v. United States*, 790 F.2d 938, 942 (D.C. Cir. 1986) (Scalia, J.)); *see also Rochester Tel. Corp. v. United States*, 307 U.S. 125, 130 (1939) (agency orders "setting a case for hearing despite a challenge to its jurisdiction…are not reviewable"); *Total Gas & Power N. Am., Inc. v. FERC*, 859 F.3d 325 (5th Cir. 2017). Huawei's challenge to the initial designation must be dismissed.

V. EVEN IF THE INITIAL DESIGNATION WERE JUDICIALLY REVIEWABLE, HUAWEI'S SUBSTANTIVE CHALLENGES ARE UNAVAILING.

A. The Initial Designation Did Not Violate Huawei's Due Process Rights.

1. Huawei argues (Br. 57-63) that in initially designating it as a covered company, the Commission deprived it of due process. The existence of a deprivation is "[t]he first inquiry in every due process challenge," and a challenge may proceed "[o]nly after finding the deprivation of a protected

interest." *Am. Mfrs. Mut. Ins. Co. v. Sullivan*, 526 U.S. 40, 59 (1999). But the initial designation has not deprived Huawei of any constitutionally protected interest and has no effect on Huawei's liberty or property rights. Any such effect would flow only from a final designation. Because that process "has not yet run its course," Huawei "ha[s] not suffered any deprivation" and thus cannot assert a procedural due process claim. *Monk v. Huston*, 340 F.3d 279, 282-83 (5th Cir. 2003).

Indeed, Huawei's attempt to bring a due process challenge to the initial designation makes little sense, because the initial designation is *how* the agency provides process.[12] The initial designation provided Huawei notice of evidence in the record and the Commission's consideration of that evidence, and invited Huawei to be heard on its sufficiency or any countervailing evidence before the agency reaches any final designation. "[D]ue process is required not before the initial decision or recommendation to terminate…but instead before the termination actually occurs." *Riggins v. Goodman*, 572 F.3d 1101, 1110 (10th Cir. 2009).

[12] *Cf. Orton Motor, Inc. v. U.S. Dep't of Health & Human Servs.*, 884 F.3d 1205, 1215 (D.C. Cir. 2018) ("the mere issuance of a warning letter, absent further enforcement action…'is [not] by itself sufficient to invoke the procedural protection of the Due Process Clause'"); *see Order* n.268 (JA___) (quoting *Orton*).

By Huawei's logic, if the Commission had issued an earlier round of notice before adopting the initial designation, Huawei would have been entitled to object that *that* notice should have been preceded by an even earlier round of notice and a hearing, and so on, *ad infinitum*. But the Due Process Clause requires notice and an opportunity to be heard, not endless rounds of notice and hearing. *See, e.g.*, *Crum v. Vincent*, 493 F.3d 988, 993 (8th Cir. 2007) ("So long as one hearing will provide…a meaningful opportunity to be heard, due process does not require two hearings on the same issue."); *Blackout Sealcoating, Inc. v. Peterson*, 733 F.3d 688, 691 (7th Cir. 2013) ("The due process clause…does not require an extended to-and-fro…. One opportunity to respond was enough.").

2. Huawei's concern that the initial designation might result in harm to its "reputation" is likewise insufficient to state a cognizable due process claim.

Huawei relies (Br. 58-59) on cases holding that severe stigma *plus* some other tangible change to its legal status—the so-called "stigma-plus" test, *see Order* ¶¶102-103 (JA___-__)—can sometimes implicate due process rights. But even if Huawei could establish the requisite stigma, it is unable to identify any "plus." *Id.* Even assuming that a *final* designation might have a cognizable effect on Huawei's legal status, *but see id.* ¶¶99-103 (JA___-__),

the *initial* designation has no such effect. And "[i]nvasion of an interest in reputation alone is insufficient." *Geter v. Fortenberry*, 849 F.2d 1550, 1556-57 (5th Cir. 1988) (citing *Paul v. Davis*, 424 U.S. 693 (1976)); *see also*, *e.g.*, *Siegert v. Gilley*, 500 U.S. 226, 233-34 (1991); *WMX Techs., Inc. v. Miller*, 197 F.3d 367, 373-76 (9th Cir. 1999) (en banc) (same as to loss of a business's "goodwill").

Moreover, Huawei's claim that it is severely stigmatized by the initial designation is largely unsubstantiated. There is no reason to think that any such consequences stem from *the initial designation itself*, as opposed to the underlying evidence that led the Commission to issue the initial designation; the initial designation itself broke no new ground. *Cf. Order* n.277 (JA___) ("[I]t is unclear whether the designation will create any new stigma beyond what already has been created by the NDAA and other government actions."); *id.* ¶171 (JA___) ("Many service providers have already made the business decision to purchase equipment from alternative vendors in order to avoid security risks.").

Huawei claims (Br. 59-60) that it lost business when the Commission issued the *NPRM*—suggesting that customers surmised that if the proposed rule were adopted, Huawei might be affected—but it presents no evidence that customers who stuck with it at that time suddenly abandoned it after the

initial designation. After all, as the declarations cited by Huawei indicate (*see id.*), information suggesting that Huawei might be a national security threat was already known to its customers when the Commission issued the *NPRM*, and the subsequent decision to issue an initial designation and conduct a full investigation is unlikely to have been a surprise.

c. Even if the Due Process Clause were implicated here by the initial designation, Huawei received all of the process it was due. Prior to the initial designation, the *NPRM* discussed longstanding concerns about the potential threats posed by Huawei and ZTE. *NPRM* ¶¶3-6 (JA___-__); *see Order* ¶¶24, 43, 95-96 (JA___, ___, ___-__). It pointed to assessments issued by Congress and the Executive Branch highlighting much of the same evidence the *Order* cites as support for a full investigation. *Id.* In response, Huawei fully and repeatedly presented its views to the agency, submitting dozens of filings spanning many hundreds of pages. *See Order* ¶43 & n.123 (JA___-__); *id.* ¶95 & n.261 (JA___).

Huawei fails to show that any further process was required here. To determine what process is due, courts weigh the private interest at stake, and the probable value (if any) of additional process in protecting that interest, against the government's interest and the fiscal and administrative burdens that additional process would entail. *Caine v. Hardy*, 943 F.2d 1406, 1412

(5th Cir. 1991) (en banc) (citing *Mathews v. Eldridge*, 424 U.S. 319, 335 (1976)). Here, the government's interest in issuing the initial designation and moving swiftly to conduct a full and expeditious investigation of a possible national security threat to critical domestic communications networks is compelling. *See Order* ¶¶83-84, 168-172 (JA___-__, ___-__). Given the magnitude of that interest, "[n]ot even an informal hearing…must precede a deprivation undertaken to protect the public safety." *Caine*, 943 F.2d at 1412.

By contrast, the private interests at stake from an initial designation are minimal, since the initial designation does not restrict Huawei's legal rights or obligations, and requiring additional process before an initial designation would add little value when Huawei will receive full process before any final designation. Huawei has not shown that it would be worth the additional burden to require additional process at this interlocutory stage.

B. The Initial Designation Is Not Impermissibly Retroactive.

There is no basis for Huawei's contention that the initial designation, issued at the same time as the USF rule, is impermissibly retroactive because it imposes "new disabilities" based on past conduct. Br. 65 (quoting *Nat'l Min. Ass'n v. Dep't of Interior*, 177 F.3d 1, 8 (D.C. Cir. 1999)). First, the initial designation does not impose *any* disability, much less a retroactive one,

because Huawei equipment will only be excluded from USF reimbursement if there is a final designation.

Regardless, no part of the rule operates retroactively. In a retroactivity analysis, a court must identify the conduct regulated to determine whether it occurs before or after adoption. *See, e.g.*, *Landgraf v. USI Film Prod.*, 511 U.S. 244, 280 (1994) ("[T]he court's first task is to determine whether Congress has expressly prescribed the statute's proper reach."); *McAndrews v. Fleet Bank of Mass., N.A.*, 989 F.2d 13, 16 (1st Cir. 1993) (citing *Cox v. Hart*, 260 U.S. 427, 434-35 (1922)) ("whether a statute's application in a particular situation is prospective or retroactive depends upon whether the conduct that allegedly triggers the statute's application occurs before or after the law's effective date"). Here, the FCC's rule has two principal components, both of which only apply prospectively.

First, the rule prohibits carriers from using Universal Service support to obtain equipment that the Commission determines poses a threat to network or supply chain integrity. That rule does not apply to any funds requested or received prior to the rule's adoption; it contains no provision for a "clawback." The rule applies prospectively only to future funding requests. Second, the rule provides a framework for the Commission to designate companies whose service or equipment now "*poses* a national security

threat." 47 C.F.R. §54.9 (emphasis added). That is, the designation process focuses on the entity's current and future risk to American networks. And even a final designation may be reversed if the company conforms its conduct to remove any security risks identified. *Order* ¶42 (JA__). Because regulated parties "know what the law is and [can] conform their conduct accordingly," *Landgraf*, 511 U.S. at 265, the rule is not retroactive.

While a designation proceeding may consider past behavior, "[a] regulation is not made retroactive merely because it draws upon antecedent facts for its operation." *Bell Atl. Tel. Cos. v. FCC*, 79 F.3d 1195, 1207 (D.C. Cir. 1996) (internal quotation marks omitted); *see also Regions Hosp. v. Shalala*, 522 U.S. 448, 456 (1998); *Ass'n of Accredited Cosmetology Schs. v. Alexander*, 979 F.2d 859, 865 (D.C. Cir. 1992). In particular, regulations are not "improperly retroactive" if they "contemplate only the use of past information for subsequent decisionmaking." *Adm'rs of Tulane Educ. Fund v. Shalala*, 987 F.2d 790, 798 (D.C. Cir. 1993). A covered company's exclusion from USF funding will ultimately be based on the company's *present* and *continued* risk to network security, not on any specific past conduct. *Cf. Fernando-Vargas v. Gonzales*, 548 U.S. 30, 41-43 (2006) (statute applied prospectively to aliens who "chose to remain" in country after enactment date, even though illegal reentry occurred prior to enactment).

A rule can also be retroactive if it "takes away or impairs vested rights acquired under existing laws" or otherwise "attaches a new disability…in respect to transactions or considerations already past." *Landgraf*, 511 U.S. at 269. But none of those considerations apply here, where "the Commission has not increased any carrier's liability for past transactions." *Bell Atl.*, 79 F.3d at 1207. Indeed, the rules "do not *create* any liability" because they "do not regulate past transactions." *Id.* Instead, they use past facts to evaluate current and potential future risk. *See Accredited Cosmetology*, 979 F.2d at 863-66 (rule that based schools' loan eligibility on past default rate was not retroactive because it did not "undo[] past eligibility," but merely "look[ed] at schools' past default rates in determining future eligibility").

The cases on which Huawei relies (Br. 64) are inapposite because they involved rules seeking to punish or remedy past behavior, as opposed to evaluating and mitigating present and future risk. *See*, *e.g.*, *Bowen v. Georgetown Univ. Hosp.*, 488 U.S. 204, 208 (1988) (retroactive cost limits and offsets for Medicare services already rendered); *Nat'l Min. Ass'n*, 177 F.3d at 8 (blocking permits for mines with unremedied past violations); *Rock of Ages Corp. v. Sec'y of Labor*, 170 F.3d 148, 159 (2d Cir. 1999) (fine for conduct that occurred before rule); *United States v. AMC Entm't, Inc.*, 549 F.3d 760, 762 (9th Cir. 2008) (injunction for movie theatres to comply with

ADA requirements that were unclear when theaters were built). And *Smith v. Doe*, 538 U.S. 84, 105-06 (2003), cited by Huawei, actually upheld a sex offender registry because it was "nonpunitive," so its "retroactive application [did] not violate the Ex Post Facto Clause." Because a designation under the *Order* is prophylactic rather than punitive, it too is not impermissibly retroactive.

C. The Initial Designation Is Supported By Ample Evidence.

Even if the initial designation were subject to judicial review, the *Order* identifies ample basis for the Commission to investigate whether Huawei's equipment and services could be exploited by the Chinese government.[13] In deciding whether to issue an initial designation and conduct an investigation, the Commission "will base its determination on the totality of the evidence," including "determinations by the Commission, Congress or the President that an entity poses a national security threat; determinations by

[13] The factual basis for a designation is subject to review only for substantial evidence, which "involves 'more than a scintilla, less than a preponderance, and is such relevant evidence as a reasonable mind might accept as adequate to support a conclusion." *Worldcall Interconnect, Inc. v. FCC*, 907 F.3d 810, 817 (5th Cir. 2018). In making adjudicatory determinations, the FCC is "free to fashion [its] own rules of procedure and to pursue methods of inquiry" needed to act effectively, and it need not adhere to the same evidentiary or procedural rules that a court might apply. *Pottsville*, 309 U.S. at 142-44.

other executive agencies that an entity poses a national security threat; and, any other available evidence, whether open source or classified, that an entity poses a national security threat." *Order* ¶41 (JA___). The Commission reasonably found that the evidence supports the initial designation here.

1. The record reflects that the Chinese government and its agents have engaged in actions that threaten the national security of the United States. The United States and its allies have identified "numerous instances where the Chinese government has engaged in malicious acts," including state-sponsored compromise of service providers. *Order* ¶44 (JA___) (citing RWR 2019 Report at 8). Other authorities document China's "notorious reputation for persistent industrial espionage, and in particular for close collaboration between government and Chinese industry." *Id.* (citing NATO Cyber Defence Centre Paper at 7, 10). The *Order* identifies numerous examples of "the Chinese government's involvement in computer intrusion and attacks as well as economic espionage." *Order* ¶46 (JA___); *see id.* n.141 (JA___) (collecting examples).

2. The *Order* identifies ample reason to investigate whether Huawei is susceptible to Chinese government influence or control. As explained above, record evidence suggests that Huawei maintains close ties to the Chinese government and military apparatus. *Order* ¶¶48-51 (JA___-__); *see supra*

p. 19. And documents obtained by the United States government from former Huawei employees "show[] that Huawei provides special network services to an entity…believe[d] to be an elite cyber-warfare unit" in the Chinese military. *Order* ¶50 (JA__).

There is also reason to investigate whether Huawei is financially beholden to the Chinese government. Analysts have found that Huawei "'is treated as a state-owned enterprise'" and "benefit[s] from vast subsidies from the Chinese government." *Order* ¶51 (JA___). In response to past investigations of its financial ties, Huawei "has refused to answer questions about its ownership and governance." *Id.*

More generally, the record suggests that "the Chinese government…exercises strong control over commercial entities, permitting the government, including state intelligence agencies, to demand that private communications sector entities cooperate with any governmental requests, which could involve revealing customer information, including network traffic information." *Order* ¶46 (JA___). As explained above, China's National Intelligence Law requires citizens and organizations to support and assist state intelligence work with punishment for non-cooperation. *Id.* The law also "allows Chinese intelligence agencies to take control of an

organization's facilities, including communications equipment," both inside and outside of China. *Id.*[14]

All of this evidence justifies the Commission's concern over whether "Chinese intelligence agencies have opportunities to tamper with [Huawei's] products in both the design and manufacturing processes," as the HPSCI concluded, and whether the Chinese government's access "could be exploited for malicious activity." *Order* ¶45 (JA___).

3. Cybersecurity firms examining Huawei's equipment have found significant vulnerabilities. One study "found that over half of the Huawei firmware images analyzed had at least one potential backdoor that could allow an attacker with knowledge of the firmware to log into the device." *Order* ¶54 (JA___) (citing Finite State Supply Chain Assessment at 3). It further found that Huawei "continues to make firmware updates without addressing these vulnerabilities." *Id.* These vulnerabilities are compounded, another report concluded, by "[t]he enormous range of products and services

[14] Although Huawei's brief disputes (at 70-72) these interpretations of Chinese law, the FCC found that Huawei's similar arguments below "ignore[] the Chinese government's authoritarian nature, lack of sufficient judicial checks, and its history of industrial espionage." *Order* ¶50 & n.146 (JA__ & __); *id.* ¶ 49 (JA__) ("the nature of the Chinese system 'recognizes no limits to government power'"). Moreover, even if the National Intelligence Law might be interpreted more narrowly, the record at minimum showed a serious risk that supports further investigation. *See Order* ¶56 (JA___-__).

offered by Huawei" that could give it access to "a nearly unimaginable amount of data for one company to possess." *Id.* ¶56 (JA___) (quoting Priscilla Moriuchi, *The New Cyber Insecurity: Geopolitical and Supply Chain Risks from the Huawei Monoculture* (2019)). The record before the Commission indicates that "multiple organizations have independently found similar, substantial security vulnerabilities in [Huawei's] products." *Id.* ¶57 (JA___) (internal quotation marks omitted).

4. The Commission's decision to issue an initial designation also was consistent with the actions and views of Congress, other Executive Branch agencies, and international allies.

The bipartisan HPSCI report warned of the security risks posed by Huawei's and ZTE's close ties to the Chinese government, recommending that U.S. government agencies and their contractors avoid the companies' equipment. *Order* ¶7 (JA___). The U.S. Government Accountability Office has likewise warned of "the potential security risks of foreign-manufactured equipment in commercial communications networks." *Id.* ¶9 (JA___). Congress effectively codified those concerns in limiting the use of Huawei and ZTE equipment in the 2018 and 2019 National Defense Authorization Acts. *See id.* ¶¶12-13 (JA___).

In February 2018, the leaders of all six U.S. intelligence agencies warned against purchasing equipment or services from Huawei in light of its close ties to the Chinese government. *Order* ¶52 (JA___-__). The U.S. Department of Justice filed a letter in this proceeding further detailing Huawei's demonstrated disregard for U.S. law. *Id.* ¶52 (JA___); *see id.* n.159 (JA___) (noting "criminal charges against Huawei for, among other things, violations of the U.S. embargo on Iran, bank fraud, obstruction of justice, trade secret theft, and fraud").

The *Order* further observes that "several of the United States' closest allies"—including Australia, Japan, and New Zealand— "have concluded that the risk posed by Huawei equipment and systems is too great to bear." *Order* ¶53 (JA___); *accord id.* n.160 (JA___). A report by the Parliament of the United Kingdom has similarly warned that "the Chinese State may be able to exploit any vulnerability in Huawei's equipment in order to…provide them with an attractive espionage opportunity." *Order* ¶55 (JA___) (internal quotation marks omitted). A United Kingdom oversight board later "sounded the alarm about the risks associated with Huawei's engineering processes," reporting that "Huawei had made no substantive gains in the remediation of issues reported in the previous year" and that "the Oversight Board has not

yet seen anything to give it confidence in Huawei's capacity to…address[] these underlying defects." *Id.* (internal quotation marks omitted).

This evidence, taken collectively, raised significant concerns that justified further inquiry by the agency. *See Order* ¶45.

D. Huawei Has Not Demonstrated Improper Political Influence or Prejudgment.

The extensive record fully justified the agency's decision to initially designate Huawei, and there is no legal merit to Huawei's argument that the FCC instead was "pandering to the Commission's benefactors in Congress." Br. 82. Unlike the "unusual" circumstances of *Dep't of Commerce v. New York*, 139 S. Ct. 2551, 2576 (2019), there is nothing "contrived" about the FCC's stated reasons for the rule and Huawei's designation, especially in light of the Executive Branch's longstanding concern with network security, and with Huawei in particular.

In any event, it is "entirely proper for Congressional representatives vigorously to represent the interest of their constituents," so long as they do not undermine the purpose of the statute or applicable rules of procedure. *Sierra Club v. Costle*, 657 F.2d 298, 409 (D.C. Cir. 1981). As this Court stated, "[i]t would be unrealistic to require that agencies turn a deaf ear to comments from members of Congress" during a rulemaking, and "an agency's patient audience to a member of Congress will not by itself

constitute the injection of an extraneous factor." *DCP Farms v. Yeutter*, 957 F.2d 1183, 1188 (5th Cir. 1992). "To hold otherwise would deprive the agencies of legitimate sources of information and call into question the validity of nearly every controversial rulemaking." *Costle*, 657 F.2d at 410. Huawei has offered no evidence that congressional pressure caused the agency to consider factors outside the statute in adopting the rule. *DCP Farms*, 957 F.2d at 1188.

Nor has Huawei shown improper influence on the decision to initially designate Huawei. Again, that decision is not final, and so not judicially reviewable, whatever the basis for Huawei's challenge. *See Standard Oil*, 449 U.S. at 239 (allegation that complaint was brought under "political pressure" was not final and so not reviewable); *DCP Farms*, 957 F.2d at 1189 ("To the extent that DCP Farms believes that extraneous factors were considered in the USDA's initial determination, it may make that argument in its appeal of the Deputy Administrator's decision.").

Even if the initial designation were reviewable, Huawei would need to show Congressional influence during an actual adjudication. In a similar case, this Court found there was nothing improper about a congressional letter urging agency officials to "carefully review" petitioners' case alleging fraudulent benefit claims. *DCP Farms*, 957 F.2d at 1188. There, as here,

Congressional contact occurred during the phase when the agency made an "initial determination" which would then lead to a hearing—*i.e.*, "before any proceeding which could be considered judicial or quasi-judicial." *Id.* at 1187. Because the congressional communication "was concerned about the administration of a congressionally created program," and "was part of a larger policy debate," the Court found nothing improper and was "unwilling to so dramatically restrict communications between Congress and the executive agencies over policy issues." *Id.*[15]

CONCLUSION

The petition for review should be dismissed as to Huawei's challenge to the rule because it is not ripe and as to the initial designation because it is not final. Should the Court disagree, the petition should be denied.

[15] Huawei also implies that the Commission "prejudged" the outcome of this proceeding. Br. 83-84. To be sure, individual Commissioners expressed opinions publicly on the rulemaking portion of this matter, but Huawei does not attempt to show, as it must, that the Commissioners' minds were "irrevocably closed or [that] there was an actual bias." *DCP Farm*, 957 F.2d at 1188. And, again, the designation portion of this proceeding is not yet final, much less prejudged.

Respectfully submitted,

JOSEPH H. HUNT
ASSISTANT ATTORNEY GENERAL

SHARON SWINGLE
DENNIS FAN
CIVIL DIVISION, APPELLATE STAFF

UNITED STATES
DEPARTMENT OF JUSTICE
WASHINGTON, D.C. 20530

THOMAS M. JOHNSON, JR.
GENERAL COUNSEL

ASHLEY S. BOIZELLE
DEPUTY GENERAL COUNSEL

JACOB M. LEWIS
ASSOCIATE GENERAL COUNSEL

/s/ Matthew J. Dunne

MATTHEW J. DUNNE
SCOTT M. NOVECK
COUNSEL

FEDERAL COMMUNICATIONS
COMMISSION
WASHINGTON, D.C. 20554
(202) 418-1740

June 1, 2020

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMIT

Certificate of Compliance With Type-Volume Limitation,
Typeface Requirements and Type Style Requirements

1. This document complies with the type-volume limit of Fed. R. App. P. 32(a)(7)(B) because, excluding the parts of the document exempted by Fed. R. App. P. 32(f):

   ☒ this document contains 16972 words, *or*

   ☐ this document uses a monospaced typeface and contains _ lines of text.

2. This document complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because:

   ☒ this document has been prepared in a proportionally spaced typeface using Microsoft Word 365 in 14-point Times New Roman, *or*

   ☐ this document has been prepared in a monospaced spaced typeface using _____ with _____.

s/ Matthew J. Dunne

Matthew J. Dunne
Counsel
Federal Communications Commission
Washington, D.C. 20554
(202) 418-1740

CERTIFICATE OF FILING AND SERVICE

I, Matthew J. Dunne, hereby certify that on June 1, 2020, I filed the foregoing Brief for Respondents' with the Clerk of the Court for the United States Court of Appeals for the Fifth Circuit using the electronic CM/ECF system. Participants in the case who are registered CM/ECF users will be served by the CM/ECF system.

s/ Matthew J. Dunne

Matthew J. Dunne
Counsel
Federal Communications Commission
Washington, D.C. 20554
(202) 418-1740

Statutory Addendum

CONTENTS

47 U.S.C. § 151

§ 151. Purposes of chapter; Federal Communications Commission created

For the purpose of regulating interstate and foreign commerce in communication by wire and radio so as to make available, so far as possible, to all the people of the United States, without discrimination on the basis of race, color, religion, national origin, or sex, a rapid, efficient, Nation-wide, and world-wide wire and radio communication service with adequate facilities at reasonable charges, for the purpose of the national defense, for the purpose of promoting safety of life and property through the use of wire and radio communications, and for the purpose of securing a more effective execution of this policy by centralizing authority heretofore granted by law to several agencies and by granting additional authority with respect to interstate and foreign commerce in wire and radio communication, there is created a commission to be known as the "Federal Communications Commission", which shall be constituted as hereinafter provided, and which shall execute and enforce the provisions of this chapter.

47 U.S.C. § 214

§ 214. Extension of lines or discontinuance of service; certificate of public convenience and necessity

(a) Exceptions; temporary or emergency service or discontinuance of service; changes in plant, operation or equipment

No carrier shall undertake the construction of a new line or of an extension of any line, or shall acquire or operate any line, or extension thereof, or shall engage in transmission over or by means of such additional or extended line, unless and until there shall first have been obtained from the Commission a certificate that the present or future public convenience and necessity require or will require the construction, or operation, or construction and operation, of such additional or extended line: *Provided*, That no such certificate shall be required under this section for the construction, acquisition, or operation of (1) a line within a single State unless such line constitutes part of an interstate line, (2) local, branch, or terminal lines not exceeding ten miles in length, or (3) any line acquired under section 221 of this title: *Provided further*, That the Commission may, upon appropriate request being made, authorize temporary or emergency service, or the supplementing of existing facilities, without regard to the provisions of this section. No carrier shall discontinue, reduce, or impair service to a community, or part of a community, unless and until there shall first have been obtained from the Commission a certificate that neither the present nor future public convenience and necessity will be adversely affected thereby; except that the Commission may, upon appropriate request being made, authorize temporary or emergency discontinuance, reduction, or impairment of service, or partial discontinuance, reduction, or impairment of service, without regard to the provisions of this section. As used in this section the term "line" means any channel of communication established by the use of appropriate equipment, other than a channel of communication established by the interconnection of two or more existing channels: *Provided, however*, That nothing in this section shall be construed to require a certificate or other authorization from the Commission for any installation, replacement, or other changes in plant, operation, or equipment, other than new construction, which will not impair the adequacy or quality of service provided.

(b) Notification of Secretary of Defense, Secretary of State, and State Governor

Upon receipt of an application for any such certificate, the Commission shall cause notice thereof to be given to, and shall cause a copy of such application to be filed with, the Secretary of Defense, the Secretary of State (with respect to such applications involving service to foreign points), and the Governor of each State in which such line is proposed to be constructed, extended, acquired, or operated, or in which such discontinuance, reduction, or impairment of service is proposed, with the right to those notified to be heard; and the Commission may require such published notice as it shall determine.

(c) Approval or disapproval; injunction

The Commission shall have power to issue such certificate as applied for, or to refuse to issue it, or to issue it for a portion or portions of a line, or extension thereof, or discontinuance, reduction, or impairment of service, described in the application, or for the partial exercise only of such right or privilege, and may attach to the issuance of the certificate such terms and conditions as in its judgment the public convenience and necessity may require. After issuance of such certificate, and not before, the carrier may, without securing approval other than such certificate, comply with the terms and conditions contained in or attached to the issuance of such certificate and proceed with the construction, extension, acquisition, operation, or discontinuance, reduction, or impairment of service covered thereby. Any construction, extension, acquisition, operation, discontinuance, reduction, or impairment of service contrary to the provisions of this section may be enjoined by any court of competent jurisdiction at the suit of the United States, the Commission, the State commission, any State affected, or any party in interest.

(d) Order of Commission; hearing; penalty

The Commission may, after full opportunity for hearing, in a proceeding upon complaint or upon its own initiative without complaint, authorize or require by order any carrier, party to such proceeding, to provide itself with adequate facilities for the expeditious and efficient performance of its service as a common carrier and to extend its line or to establish a public office; but no such authorization or order shall be made unless the Commission finds, as to such provision of facilities, as to such establishment of public offices, or as to such extension, that it is reasonably required in the interest of public convenience and necessity, or as to such extension or facilities that the expense involved therein will not impair the ability of the carrier to perform its duty to the public. Any carrier which refuses or neglects to comply with any order of the Commission made in pursuance of this subsection shall forfeit to the United States $1,200 for each day during which such refusal or neglect continues.

* * *

47 U.S.C. § 254

§ 254. Universal service

(a) Procedures to review universal service requirements

(1) Federal-State Joint Board on universal service

Within one month after February 8, 1996, the Commission shall institute and refer to a Federal-State Joint Board under section 410(c) of this title a proceeding to recommend changes to any of its regulations in order to implement sections 214(e) of this title and this section, including the definition of the services that are supported by Federal universal service support mechanisms and a specific timetable for completion of such recommendations. In addition to the members of the Joint Board required under section 410(c) of this title, one member of such Joint Board shall be a State-appointed utility consumer advocate nominated by a national organization of State utility consumer advocates. The Joint Board shall, after notice and opportunity for public comment, make its recommendations to the Commission 9 months after February 8, 1996.

(2) Commission action

The Commission shall initiate a single proceeding to implement the recommendations from the Joint Board required by paragraph (1) and shall complete such proceeding within 15 months after February 8, 1996. The rules established by such proceeding shall include a definition of the services that are supported by Federal universal service support mechanisms and a specific timetable for implementation. Thereafter, the Commission shall complete any proceeding to implement subsequent recommendations from any Joint Board on universal service within one year after receiving such recommendations.

(b) Universal service principles

The Joint Board and the Commission shall base policies for the preservation and advancement of universal service on the following principles:

(1) Quality and rates

Quality services should be available at just, reasonable, and affordable rates.

(2) Access to advanced services

Access to advanced telecommunications and information services should be provided in all regions of the Nation.

(3) Access in rural and high cost areas

Consumers in all regions of the Nation, including low-income consumers and those in rural, insular, and high cost areas, should have access to telecommunications and information services, including interexchange services and advanced

telecommunications and information services, that are reasonably comparable to those services provided in urban areas and that are available at rates that are reasonably comparable to rates charged for similar services in urban areas.

(4) Equitable and nondiscriminatory contributions

All providers of telecommunications services should make an equitable and nondiscriminatory contribution to the preservation and advancement of universal service.

(5) Specific and predictable support mechanisms

There should be specific, predictable and sufficient Federal and State mechanisms to preserve and advance universal service.

(6) Access to advanced telecommunications services for schools, health care, and libraries

Elementary and secondary schools and classrooms, health care providers, and libraries should have access to advanced telecommunications services as described in subsection (h).

(7) Additional principles

Such other principles as the Joint Board and the Commission determine are necessary and appropriate for the protection of the public interest, convenience, and necessity and are consistent with this chapter.

(c) Definition

(1) In general

Universal service is an evolving level of telecommunications services that the Commission shall establish periodically under this section, taking into account advances in telecommunications and information technologies and services. The Joint Board in recommending, and the Commission in establishing, the definition of the services that are supported by Federal universal service support mechanisms shall consider the extent to which such telecommunications services--

(A) are essential to education, public health, or public safety;

(B) have, through the operation of market choices by customers, been subscribed to by a substantial majority of residential customers;

(C) are being deployed in public telecommunications networks by telecommunications carriers; and

(D) are consistent with the public interest, convenience, and necessity.

(2) Alterations and modifications

The Joint Board may, from time to time, recommend to the Commission modifications in the definition of the services that are supported by Federal universal service support mechanisms.

(3) Special services

In addition to the services included in the definition of universal service under paragraph (1), the Commission may designate additional services for such support mechanisms for schools, libraries, and health care providers for the purposes of subsection (h).

(d) Telecommunications carrier contribution

Every telecommunications carrier that provides interstate telecommunications services shall contribute, on an equitable and nondiscriminatory basis, to the specific, predictable, and sufficient mechanisms established by the Commission to preserve and advance universal service. The Commission may exempt a carrier or class of carriers from this requirement if the carrier's telecommunications activities are limited to such an extent that the level of such carrier's contribution to the preservation and advancement of universal service would be de minimis. Any other provider of interstate telecommunications may be required to contribute to the preservation and advancement of universal service if the public interest so requires.

(e) Universal service support

After the date on which Commission regulations implementing this section take effect, only an eligible telecommunications carrier designated under section 214(e) of this title shall be eligible to receive specific Federal universal service support. A carrier that receives such support shall use that support only for the provision, maintenance, and upgrading of facilities and services for which the support is intended. Any such support should be explicit and sufficient to achieve the purposes of this section.

47 U.S.C. § 310

§ 310. License ownership restrictions

(a) Grant to or holding by foreign government or representative

The station license required under this chapter shall not be granted to or held by any foreign government or the representative thereof.

(b) Grant to or holding by alien or representative, foreign corporation, etc.

No broadcast or common carrier or aeronautical en route or aeronautical fixed radio station license shall be granted to or held by--

(1) any alien or the representative of any alien;

(2) any corporation organized under the laws of any foreign government;

(3) any corporation of which more than one-fifth of the capital stock is owned of record or voted by aliens or their representatives or by a foreign government or representative thereof or by any corporation organized under the laws of a foreign country;

(4) any corporation directly or indirectly controlled by any other corporation of which more than one-fourth of the capital stock is owned of record or voted by aliens, their representatives, or by a foreign government or representative thereof, or by any corporation organized under the laws of a foreign country, if the Commission finds that the public interest will be served by the refusal or revocation of such license.

(c) Authorization for aliens licensed by foreign governments; multilateral or bilateral agreement to which United States and foreign country are parties as prerequisite

In addition to amateur station licenses which the Commission may issue to aliens pursuant to this chapter, the Commission may issue authorizations, under such conditions and terms as it may prescribe, to permit an alien licensed by his government as an amateur radio operator to operate his amateur radio station licensed by his government in the United States, its possessions, and the Commonwealth of Puerto Rico provided there is in effect a multilateral or bilateral agreement, to which the United States and the alien's government are parties, for such operation on a reciprocal basis by United States amateur radio operators. Other provisions of this chapter and of subchapter II of chapter 5, and chapter 7, of Title 5 shall not be applicable to any request or application for or modification, suspension, or cancellation of any such authorization.

(d) Assignment and transfer of construction permit or station license

No construction permit or station license, or any rights thereunder, shall be transferred, assigned, or disposed of in any manner, voluntarily or involuntarily, directly or indirectly, or by transfer of control of any corporation holding such permit or license, to any person except upon application to the Commission and upon finding by the Commission that the public interest, convenience, and necessity will be served thereby. Any such application shall be disposed of as if the proposed transferee or assignee were making application under section 308 of this title for the permit or license in question; but in acting thereon the Commission may not consider whether the public interest, convenience, and necessity might be served by the transfer, assignment, or disposal of the permit or license to a person other than the proposed transferee or assignee.

(e) Administration of regional concentration rules for broadcast stations

(1) In the case of any broadcast station, and any ownership interest therein, which is excluded from the regional concentration rules by reason of the savings provision for existing facilities provided by the First Report and Order adopted March 9, 1977 (docket No. 20548; 42 Fed. Reg. 16145), the exclusion shall not terminate solely by reason of changes made in the technical facilities of the station to improve its service.

(2) For purposes of this subsection, the term "regional concentration rules" means the provisions of sections 73.35, 73.240, and 73.636 of title 47, Code of Federal Regulations (as in effect June 1, 1983), which prohibit any party from directly or indirectly owning, operating, or controlling three broadcast stations in one or several services where any two of such stations are within 100 miles of the third (measured city-to-city), and where there is a primary service contour overlap of any of the stations.

47 U.S.C. § 1003

§ 1003. Notices of capacity requirements

(a) Notices of maximum and actual capacity requirements

(1) In general

Not later than 1 year after October 25, 1994, after consulting with State and local law enforcement agencies, telecommunications carriers, providers of telecommunications support services, and manufacturers of telecommunications equipment, and after notice and comment, the Attorney General shall publish in the Federal Register and provide to appropriate telecommunications industry associations and standard-setting organizations--

(A) notice of the actual number of communication interceptions, pen registers, and trap and trace devices, representing a portion of the maximum capacity set forth under subparagraph (B), that the Attorney General estimates that government agencies authorized to conduct electronic surveillance may conduct and use simultaneously by the date that is 4 years after October 25, 1994; and

(B) notice of the maximum capacity required to accommodate all of the communication interceptions, pen registers, and trap and trace devices that the Attorney General estimates that government agencies authorized to conduct electronic surveillance may conduct and use simultaneously after the date that is 4 years after October 25, 1994.

(2) Basis of notices

The notices issued under paragraph (1)--

(A) may be based upon the type of equipment, type of service, number of subscribers, type or size or carrier, nature of service area, or any other measure; and

(B) shall identify, to the maximum extent practicable, the capacity required at specific geographic locations.

(b) Compliance with capacity notices

(1) Initial capacity

Within 3 years after the publication by the Attorney General of a notice of capacity requirements or within 4 years after October 25, 1994, whichever is longer, a telecommunications carrier shall, subject to subsection (e), ensure that its systems are capable of--

(A) accommodating simultaneously the number of interceptions, pen registers, and trap and trace devices set forth in the notice under subsection (a)(1)(A); and

(B) expanding to the maximum capacity set forth in the notice under subsection (a)(1)(B).

(2) Expansion to maximum capacity

After the date described in paragraph (1), a telecommunications carrier shall, subject to subsection (e), ensure that it can accommodate expeditiously any increase in the actual number of communication interceptions, pen registers, and trap and trace devices that authorized agencies may seek to conduct and use, up to the maximum capacity requirement set forth in the notice under subsection (a)(1)(B).

(c) Notices of increased maximum capacity requirements

(1) Notice

The Attorney General shall periodically publish in the Federal Register, after notice and comment, notice of any necessary increases in the maximum capacity requirement set forth in the notice under subsection (a)(1)(B).

(2) Compliance

Within 3 years after notice of increased maximum capacity requirements is published under paragraph (1), or within such longer time period as the Attorney General may specify, a telecommunications carrier shall, subject to subsection (e), ensure that its systems are capable of expanding to the increased maximum capacity set forth in the notice.

(d) Carrier statement

Within 180 days after the publication by the Attorney General of a notice of capacity requirements pursuant to subsection (a) or (c), a telecommunications carrier shall submit to the Attorney General a statement identifying any of its systems or services that do not have the capacity to accommodate simultaneously the number of interceptions, pen registers, and trap and trace devices set forth in the notice under such subsection.

(e) Reimbursement required for compliance

The Attorney General shall review the statements submitted under subsection (d) and may, subject to the availability of appropriations, agree to reimburse a telecommunications carrier for costs directly associated with modifications to attain such capacity requirement that are determined to be reasonable in accordance with section 1008(e) of this title. Until the Attorney General agrees to reimburse such carrier for such modification, such carrier shall be considered to be in compliance with the capacity notices under subsection (a) or (c).

47 U.S.C. § 1004

§ 1004. Systems security and integrity

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 acting in accordance with regulations prescribed by the Commission.

UNITED STATES PUBLIC LAWS
116th Congress - Second Session
PL 116–124
March 12, 2020

SECURE AND TRUSTED COMMUNICATIONS NETWORKS ACT OF 2019

An Act To prohibit certain Federal subsidies from being used to purchase communications equipment or services posing national security risks, to provide for the establishment of a reimbursement program for the replacement of communications equipment or services posing such risks, and for other purposes.
Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,
T. 47 ch. 15 prec. § 1601

SECTION 1. SHORT TITLE.

This Act may be cited as the "Secure and Trusted Communications Networks Act of 2019".

SEC. 2. DETERMINATION OF COMMUNICATIONS EQUIPMENT OR SERVICES POSING NATIONAL SECURITY RISKS.

(a) PUBLICATION OF COVERED COMMUNICATIONS EQUIPMENT OR SERVICES LIST.—Not later than 1 year after the date of the enactment of this Act, the Commission shall publish on its website a list of covered communications equipment or services.
(b) PUBLICATION BY COMMISSION.—The Commission shall place on the list published under subsection (a) any communications equipment or service, if and only if such equipment or service—
(1) is produced or provided by any entity, if, based exclusively on the determinations described in paragraphs (1) through (4) of subsection (c), such equipment or service produced or provided by such entity poses an unacceptable risk to the national security of the United States or the security and safety of United States persons; and
(2) is capable of—
(A) routing or redirecting user data traffic or permitting visibility into any user data or packets that such equipment or service transmits or otherwise handles;
(B) causing the network of a provider of advanced communications service to be disrupted remotely; or
(C) otherwise posing an unacceptable risk to the national security of the United States or the security and safety of United States persons.

(c) RELIANCE ON CERTAIN DETERMINATIONS.—In taking action under subsection (b)(1), the Commission shall place on the list any communications equipment or service that poses an unacceptable risk to the national security of the United States or the security and safety of United States persons based solely on one or more of the following determinations:
(1) A specific determination made by any executive branch interagency body with appropriate national security expertise, including the Federal Acquisition Security Council established under section 1322(a) of title 41, United States Code.
(2) A specific determination made by the Department of Commerce pursuant to Executive Order No. 13873 (84 Fed. Reg. 22689; relating to securing the information and communications technology and services supply chain).
(3) The communications equipment or service being covered telecommunications equipment or services, as defined in section 889(f)(3) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232; 132 Stat. 1918).
(4) A specific determination made by an appropriate national security agency.
(d) UPDATING OF LIST.—
(1) IN GENERAL.—The Commission shall periodically update the list published under subsection (a) to address changes in the determinations described in paragraphs (1) through (4) of subsection (c).
(2) MONITORING OF DETERMINATIONS.—The Commission shall monitor the making or reversing of the determinations described in paragraphs (1) through (4) of subsection (c) in order to place additional communications equipment or services on the list published under subsection (a) or to remove communications equipment or services from such list. If a determination described in any such paragraph that provided the basis for a determination by the Commission under subsection (b)(1) with respect to any communications equipment or service is reversed, the Commission shall remove such equipment or service from such list, except that the Commission may not remove such equipment or service from such list if any other determination described in any such paragraph provides a basis for inclusion on such list by the Commission under subsection (b)(1) with respect to such equipment or service.
(3) PUBLIC NOTIFICATION.—For each 12-month period during which the list published under subsection (a) is not updated, the Commission shall notify the public that no updates were necessary during such period to protect national security or to address changes in the determinations described in paragraphs (1) through (4) of subsection (c).

SEC. 3. PROHIBITION ON USE OF CERTAIN FEDERAL SUBSIDIES.

(a) IN GENERAL.—

(1) PROHIBITION.—A Federal subsidy that is made available through a program administered by the Commission and that provides funds to be used for the capital expenditures necessary for the provision of advanced communications service may not be used to—

(A) purchase, rent, lease, or otherwise obtain any covered communications equipment or service; or

(B) maintain any covered communications equipment or service previously purchased, rented, leased, or otherwise obtained.

(2) TIMING.—Paragraph (1) shall apply with respect to any covered communications equipment or service beginning on the date that is 60 days after the date on which the Commission places such equipment or service on the list required by section 2(a). In the case of any covered communications equipment or service that is on the initial list published under such section, such equipment or service shall be treated as being placed on the list on the date on which such list is published.

(b) COMPLETION OF PROCEEDING.—Not later than 180 days after the date of the enactment of this Act, the Commission shall adopt a Report and Order to implement subsection (a). If the Commission has, before the date of the enactment of this Act, taken action that in whole or in part implements subsection (a), the Commission is not required to revisit such action, but only to the extent such action is consistent with this section.

* * *

SEC. 9. DEFINITIONS.

In this Act:

(1) ADVANCED COMMUNICATIONS SERVICE.—The term "advanced communications service" has the meaning given the term "advanced telecommunications capability" in section 706 of the Telecommunications Act of 1996 (47 U.S.C. 1302).

(2) APPROPRIATE NATIONAL SECURITY AGENCY.—The term "appropriate national security agency" means—

(A) the Department of Homeland Security;

(B) the Department of Defense;

(C) the Office of the Director of National Intelligence;

(D) the National Security Agency; and

(E) the Federal Bureau of Investigation.

(3) COMMISSION.—The term "Commission" means the Federal Communications Commission.
(4) COMMUNICATIONS EQUIPMENT OR SERVICE.—The term "communications equipment or service" means any equipment or service that is essential to the provision of advanced communications service.
(5) COVERED COMMUNICATIONS EQUIPMENT OR SERVICE.—The term "covered communications equipment or service" means any communications equipment or service that is on the list published by the Commission under section 2(a).
(6) CUSTOMERS.—The term "customers" means, with respect to a provider of advanced communications service—
(A) the customers of such provider; and
(B) the customers of any affiliate (as defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153)) of such provider.
(7) EXECUTIVE BRANCH INTERAGENCY BODY.—The term "executive branch interagency body" means an interagency body established in the executive branch.
(8) PERSON.—The term "person" means an individual or entity.
(9) PROGRAM.—The term "Program" means the Secure and Trusted Communications Networks Reimbursement Program established under section 4(a).
(10) PROVIDER OF ADVANCED COMMUNICATIONS SERVICE.—The term "provider of advanced communications service" means a person who provides advanced communications service to United States customers.
(11) RECIPIENT.—The term "recipient" means any provider of advanced communications service the application of which for a reimbursement under the Program has been approved by the Commission, regardless of whether the provider has received reimbursement funds.
(12) REIMBURSEMENT FUNDS.—The term "reimbursement funds" means any reimbursement received under the Program.

* * *

47 C.F.R. § 54.9

§ 54.9 Prohibition on use of funds.

(a) USF support restriction No universal service support may be used to purchase, obtain, maintain, improve, modify, or otherwise support any equipment or services produced or provided by any company posing a national security threat to the integrity of communications networks or the communications supply chain.

(b) Designation of Entities Subject to Prohibition.

(1) When the Public Safety and Homeland Security Bureau (PSHSB) determines, either sua sponte or in response to a petition from an outside party, that a company poses a national security threat to the integrity of communications networks or the communications supply chain, PSHSB shall issue a public notice advising that such designation has been proposed as well as the basis for such designation.

(2) Upon issuance of such notice, interested parties may file comments responding to the initial designation, including proffering an opposition to the initial designation. If the initial designation is unopposed, the entity shall be deemed to pose a national security threat 31 days after the issuance of the notice. If any party opposes the initial designation, the designation shall take effect only if PSHSB determines that the affected entity should nevertheless be designated as a national security threat to the integrity of communications networks or the communications supply chain. In either case, PSHSB shall issue a second public notice announcing its final designation and the effective date of its final designation. PSHSB shall make a final designation no later than 120 days after release of its initial determination notice. PSHSB may, however, extend such 120–day deadline for good cause.

(3) PSHSB will act to reverse its designation upon a finding that an entity is no longer a threat to the integrity of communications networks or the communications supply chain. A designated company, or any other interested party, may submit a petition asking PSHSB to remove a designation. PSHSB shall seek the input of Executive Branch agencies and the public upon receipt of such a petition. If the record shows that a designated company is no longer a national security threat, PSHSB shall promptly issue an order reversing its designation of that company.

PSHSB may dismiss repetitive or frivolous petitions for reversal of a designation without notice and comment. If PSHSB reverses its designation, PSHSB shall issue an order announcing its decision along with the basis for its decision.

(4) PSHSB shall have discretion to revise this process or follow a different process if appropriate to the circumstances, consistent with providing affected parties an opportunity to respond and with any need to act expeditiously in individual cases.