ORAL ARGUMENT NOT YET SCHEDULED

Nos. 23-1032 & 23-1073

IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

HIKVISION USA, INC.,
DAHUA TECHNOLOGY USA INC.,

Petitioners,

v.

FEDERAL COMMUNICATIONS COMMISSION
and UNITED STATES OF AMERICA,

Respondents.

On Petitions for Review of an Order of
the Federal Communications Commission

BRIEF FOR RESPONDENTS

Brian M. Boynton
Principal Deputy Assistant Attorney General

Sharon Swingle
Casen Ross
Attorneys

U.S. DEPARTMENT OF JUSTICE
CIVIL DIVISION
950 Pennsylvania Ave. NW
Washington, DC 20530

P. Michele Ellison
General Counsel

Jacob M. Lewis
Deputy General Counsel

Sarah E. Citrin
Deputy Associate General Counsel

Matthew J. Dunne
Counsel

FEDERAL COMMUNICATIONS COMMISSION
45 L Street NE
Washington, DC 20554
(202) 418-1740
fcclitigation@fcc.gov

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

(A) **Parties and Amici.** All parties and intervenors appearing in this Court are listed in the Brief for Petitioners.

(B) **Rulings Under Review.** The petitions for review challenge the following order of the Federal Communications Commission: *Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program, Protecting Against National Security Threats to the Communications Supply Chain Through the Competitive Bidding Program*, Report and Order, Order, and Further Notice of Proposed Rulemaking, FCC 22-84, (rel. Nov. 25, 2022) ("*Order*"), *reprinted at* JA__–__.

(C) **Related Cases.** The order under review has not previously been before this Court or any other court. Respondents are aware of no other related cases within the meaning of D.C. Circuit Rule 28(a)(1)(C).

TABLE OF CONTENTS

Page

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES i
TABLE OF AUTHORITIES iv
GLOSSARY viii
INTRODUCTION 1
JURISDICTIONAL STATEMENT 3
STATEMENT OF THE ISSUES 4
PERTINENT STATUTES AND REGULATIONS 5
STATEMENT OF THE CASE 5
A. Congressional and FCC Measures to Secure the Nation's Communications Systems 5
1. Dahua and Hikvision 6
2. The National Defense Authorization Acts and the *Supply Chain Order* 7
3. Secure Networks Act 10
4. *Supply Chain Second Order* 11
B. The FCC's Equipment Authorization Program 13
C. The Notice of Proposed Rulemaking 15
D. Secure Equipment Act 16
E. *Order* on Review 17
1. Legal Authority 18
2. Confirmation of the *Supply Chain Second Order* Interpretations of Covered List 19
3. Scope of Rule 22
STANDARD OF REVIEW 26
SUMMARY OF THE ARGUMENT 27
ARGUMENT 31

TABLE OF CONTENTS
(continued)

Page

I. THE FCC ACTED WITHIN ITS AUTHORITY AND PURSUANT TO CONGRESS'S INSTRUCTION IN FORBIDDING AUTHORIZATION FOR COVERED EQUIPMENT. 31

A. The Secure Equipment Act Granted Authority for the *Order*. 32

B. Alternately, the FCC Already Had Authority for the *Order*, as Confirmed by the Secure Equipment Act. 33

II. THE FCC'S INTERPRETATION OF COVERED EQUIPMENT TO INCLUDE PETITIONERS' PRODUCTS FOR CERTAIN USES WAS REASONABLE AND APPROVED BY CONGRESS. 38

A. Most of Petitioners' Arguments About the Secure Networks Act Are Both Untimely and Foreclosed by the Secure Equipment Act. 38

B. Video Surveillance Equipment Is Essential to the Provision of Advanced Services Within the Meaning of the Secure Networks Act. 43

C. Video Surveillance Equipment Is Capable of Posing an Unacceptable Risk to National Security Within the Meaning of the Secure Networks Act. 48

D. The FCC's Interpretation of "Critical Infrastructure" Under the Statutes Is Reasonable. 52

CONCLUSION 58

TABLE OF AUTHORITIES*

Cases

Bhd. of Locomotive Engineers & Trainmen v. Fed. R.R. Admin., 972 F.3d 83 (D.C. Cir. 2020) 38

Bob Jones Univ. v. United States, 461 U.S. 574 (1983) 42

Chevron U.S.A., Inc. v. Nat. Res. Def. Council, Inc., 467 U.S. 837 (1984) 56

* *China Telecom (Ams.) Corp. v. FCC*, 57 F.4th 256 (D.C. Cir. 2022) 5, 6, 26, 35

FCC v. Prometheus Radio Project, 141 S. Ct. 1150 (2021) 26

Haig v. Agee, 453 U.S. 280 (1981) 35

Huawei Techs. USA, Inc. v. FCC, 2 F.4th 421 (5th Cir. 2021) 5, 9, 35

Jackson v. Modly, 949 F.3d 763 (D.C. Cir. 2020) 41, 42

Maine Lobstermen's Ass'n v. Nat'l Marine Fisheries Serv., 70 F.4th 582 (D.C. Cir. 2023) 37

Merrill Lynch, Pierce, Fenner & Smith, Inc. v. Curran, 456 U.S. 353 (1982) 41

NBC v. United States, 319 U.S. 190 (1943) 35

Pub. Emps. for Env't Responsibility v. EPA, -- F.4th --, 2023 WL 4714021 (D.C. Cir. July 25, 2023) 39

Rural Cellular Ass'n v. FCC, 588 F.3d 1095 (D.C. Cir. 2009) 8

Sierra Club v. EPA, 925 F.3d 490 (D.C. Cir. 2019) 39

---

* *Authorities upon which we chiefly rely are marked with asterisks.*

TABLE OF AUTHORITIES
(continued)

Page(s)

Statutes

5 U.S.C. § 706(2) 26

28 U.S.C. § 2342(1) 3

28 U.S.C. § 2344 ..... 4, 28

42 U.S.C. § 5195(c)(e) 54

47 U.S.C. § 151 ..... 5, 15, 19, 28, 34

47 U.S.C. § 154(i) 16

47 U.S.C. § 229(a)–(b) 28, 36

47 U.S.C. § 302a 14

* 47 U.S.C. § 302a(a) 14, 27, 34, 35

47 U.S.C. § 302a(b) 14

47 U.S.C. § 303(e) 14, 27, 34

47 U.S.C. § 402(a) 3

47 U.S.C. § 1004 ..... 19, 28, 36

47 U.S.C. § 1302(d)(1) 44, 45

47 U.S.C. § 1601 note 16

47 U.S.C. §§ 1601-1609 10

* Communications Assistance for Law Enforcement Act (CALEA), Pub. L. No. 103–414, 108 Stat. 4279 (1994) (codified at 47 U.S.C. § 1001 et seq.) 36

TABLE OF AUTHORITIES
(continued)

Page(s)

National Defense Authorization Act for Fiscal Year 2018, Pub. L. 115-91, 131 Stat. 1283 (2017) 7

* National Defense Authorization Act for Fiscal Year 2019, Pub. L. 115-232, 132 Stat. 1636 (2018) 8, 9, 20, 27, 47, 52

* Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 134 Stat. 158 (2020) .. 10, 11, 12, 19, 29, 33, 43, 44, 47, 48

* Secure Equipment Act of 2021, Pub. L. No. 117-55, 135 Stat. 423 (2021) 16, 17, 18, 31, 32, 37, 42

Regulations

47 C.F.R. § 1.401 41

47 C.F.R. § 1.50001(c) 22

47 C.F.R. §§ 2.801 *et seq.* 14

47 C.F.R. §§ 2.901 *et seq.* 14

47 C.F.R. § 2.901 14

47 C.F.R. §§ 2.1201 *et seq.* 14

47 C.F.R. § 54.9 9

Administrative Materials

Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, 34 FCC Rcd 11423 (2019) 9

TABLE OF AUTHORITIES
(continued)

Page(s)

* *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, 35 FCC Rcd 14284 (2020) 11, 12, 13, 19, 21, 22, 28, 30, 38, 40, 41, 42, 44, 45, 49, 50, 52

Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, 36 FCC Rcd 11958 (2021) 46, 47

Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, Notice of Proposed Rulemaking, 33 FCC Rcd 4058 (2018) 8

Public Safety and Homeland Security Bureau Announces Publication of the List of Equipment and Services Covered by Section 2 of the Secure Networks Act, 36 FCC Rcd 5534 (2021) .. 13, 24

Other Materials

BBC Panorama, *The tech flaw that lets hackers control surveillance cameras*, BBC News, June 26, 2023 51

Brian Contos, *The Secret, Insecure Life of Security Cameras*, Forbes, Mar. 1, 2023 51

Directive on Critical Infrastructure Security and Resilience, 1 Pub. Papers 106 (Feb. 12, 2013) 25, 54

National Risk Management Center, Cybersecurity and Infrastructure Security Agency, *National Critical Functions Status Update to the Critical Infrastructure Community* (2020). 25, 54

GLOSSARY

2019 NDAA	2019 National Defense Authorization Act, Pub. L. 115-232, 132 Stat. 1636
CALEA	Communications Assistance for Law Enforcement Act, Pub. L. No. 103–414, 108 Stat. 4279 (1994) (codified at 47 U.S.C. § 1001 et seq.)
NPRM	*Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program*, ET Docket No. 21–232, 36 FCC Rcd 10578 (2021) (JA__)
USF	Universal Service Fund, an FCC-administered fund that provides funds to telecommunications providers to subsidize some services

Nos. 23-1032 & 23-1073

IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

HIKVISION USA, INC.,
DAHUA TECHNOLOGY USA INC.,

Petitioners,

v.

FEDERAL COMMUNICATIONS COMMISSION
and UNITED STATES OF AMERICA,

Respondents.

On Petitions for Review of an Order of
the Federal Communications Commission

BRIEF FOR RESPONDENTS

INTRODUCTION

In recent years, Congress and the Federal Communications Commission (FCC) have acted to ensure the security of the nation's communications networks and supply chain, including by addressing potential threats from technology companies owned or influenced by the Chinese Government. In carrying out these efforts, the FCC and Congress have engaged in an extended and productive dialogue. In 2018, the FCC proposed to prohibit the use of certain subsidies to purchase

equipment made by two Chinese-government-owned technology firms, Huawei and ZTE. Congress then passed a statute—the 2019 National Defense Authorization Act (2019 NDAA)—that contained a similar prohibition covering all federal funds. Notably, that prohibition also extended specifically to video surveillance equipment from petitioners Dahua and Hikvision that was used for certain identified purposes.

After the FCC implemented this directive, Congress passed the Secure Networks Act, which ordered the agency to maintain a "Covered List" of equipment ineligible for FCC-administered funds. In doing so, Congress referred to the previous 2019 NDAA (which, again, mentioned petitioners' equipment). The FCC implemented this rule and included petitioners' equipment on its Covered List—a determination that petitioners did not challenge at that time.

The FCC then commenced a new rulemaking, proposing to alter its equipment authorization rules to forbid authorization of equipment on the Covered List, thus effectively barring the importation, sale, and marketing of such equipment altogether, not just where FCC-administered funds were used. While this rulemaking was underway, Congress passed another statute, the Secure Equipment Act, which referred to the FCC's equipment authorization proposal by name and

docket number and directed the agency to do just what had been proposed in that rulemaking. The FCC implemented Congress's directive in the *Order* on review.

Much of petitioners' challenge to the *Order* rests on the agency's interpretation of the Secured Networks Act that it had adopted when implementing the Covered List in 2020. That challenge is untimely; it is also foreclosed in light of Congress's subsequent ratification of that reading. In any case, the *Order* on review is a reasonable exercise of the authority that Congress has conferred on the FCC in the course of their dialogue on how best to protect the nation's communications infrastructure from national security threats.

JURISDICTIONAL STATEMENT

This Court has jurisdiction pursuant to 28 U.S.C. § 2342(1) and 47 U.S.C. § 402(a). The FCC issued the *Order* on November 25, 2022. (JA___). Petitioners timely filed their petitions for review on February 13 and February 14, 2023. To the extent petitioners challenge the FCC's interpretation of the Secure Networks Act, the Court lacks jurisdiction over petitioners' untimely challenge. That interpretation was set out in the *Supply Chain Second Order*, which the agency adopted in 2020; but

the petitions were filed in 2023, after the 60-day deadline to seek judicial review, see 28 U.S.C. § 2344. *See below at* II.A.

STATEMENT OF THE ISSUES

1. Whether the FCC was authorized to take the measures set out in the *Order* by either the Secure Equipment Act, or alternately, by section 302 of the Communications Act and/or section 105 of Communications Assistance for Law Enforcement Act?

2. Whether petitioners' challenges to the FCC's implementation of the Secure Networks Act, which the agency adopted in its 2020 *Supply Chain Second Order*, are untimely, or alternately foreclosed by the Secure Equipment Act?

3. If petitioners' challenges are properly before this Court, whether the FCC's interpretation of the Secure Networks Act, which found that petitioners' products are both "communications equipment" and "capable" of posing a threat to national security, was reasonable?

4. Whether, in interpreting the term "critical infrastructure" in its rules, the FCC reasonably incorporated definitions from the USA Patriot Act, a presidential policy directive, and a publication from the Department of Homeland Security?

PERTINENT STATUTES AND REGULATIONS

Pertinent statutes and regulations are set forth in the statutory addendum bound with this brief. The rules added and amended by the *Order* on review appear in Appendix A to the *Order* (JA__).

STATEMENT OF THE CASE

A. Congressional and FCC Measures to Secure the Nation's Communications Systems

Congress established the Federal Communications Commission to regulate "interstate and foreign commerce in communication by wire and radio" in order to, among other things, "promot[e] safety of life and property" and to serve "the national defense." 47 U.S.C. § 151. Indeed "national defense" is "[o]ne of the principal purposes" of the Communications Act. *China Telecom (Ams.) Corp. v. FCC*, 57 F.4th 256, 261 (D.C. Cir. 2022); *see Huawei Techs. USA, Inc. v. FCC*, 2 F.4th 421, 439–40, 443–44 (5th Cir. 2021) (upholding the FCC's authority to address communications-related national security threats).

In recent years, Congress, the FCC, and other Executive Branch entities have taken several actions to ensure the security of the nation's communications networks, including by addressing potential threats posed by some foreign companies and equipment, including especially companies owned or controlled by the Chinese Government. As this Court

has noted elsewhere, "China has augmented the level of state control over the cyber practices of Chinese companies," and recent laws "require[] Chinese companies to cooperate with state agencies on cybersecurity supervision and inspection." *China Telecom*, 57 F.4th at 263. "The Office of the Director of National Intelligence now warns of cyberattacks by the Chinese government and the potential use of Chinese information technology firms as systemic espionage platforms." *Id.* at 262–63. "The FBI [likewise] warns that no country poses a broader, more severe intelligence collection threat than China." *Id.* at 263.

1. Dahua and Hikvision

Petitioners Dahua Technology USA Inc. (Dahua) and Hikvision USA, Inc. (Hikvision) are subsidiaries of Chinese-based manufacturers of electronic video equipment. Br. iii; *see also id.* (Hikvision's largest shareholder is a state-owned entity). As Chinese companies, both are subject to Chinese national security laws. *See China Telecom,* 57 F.4th at 263.

2. The National Defense Authorization Acts and the *Supply Chain Order*

The statutory and regulatory background to this case is somewhat protracted, but an accurate understanding of that background is critical to a proper evaluation of the underlying dispute.

In December 2017, Congress enacted the National Defense Authorization Act for Fiscal Year 2018 which barred the Department of Defense from using telecommunications equipment or services produced or provided by two Chinese-government-owned and -controlled companies, Huawei Technologies Company (Huawei) and ZTE Corporation (ZTE), for certain critical programs. Pub. L. 115-91, 131 Stat. 1283, 1762, § 1656 (2017).

The FCC built upon this framework in April 2018 when it proposed to prohibit the use of subsidies from the agency's Universal Service Fund (USF) to purchase equipment or services from any communications equipment or service provider identified as posing a national security risk to communications networks or the communications supply chain. *See Protecting Against National Security Threats to the Communications*

Supply Chain Through FCC Programs, Notice of Proposed Rulemaking, 33 FCC Rcd 4058, 4058, ¶ 2 (2018).[1]

In August 2018, while the FCC's USF rulemaking was ongoing, Congress enacted the 2019 NDAA. Pub. L. 115-232, 132 Stat. 1636. This law prohibits Executive Branch agencies, including the FCC, from using federal funds to procure equipment, services, or systems that use "covered telecommunications equipment or services" as a substantial component of any system. 2019 NDAA, 132 Stat. at 1918, § 889(f)(2)-(3). The 2019 NDAA defines "covered telecommunications equipment or services" in four categories, one of which specifically refers to petitioners Hikvision and Dahua by name:

> For the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities).

---

[1] The USF is an FCC-administered fund that provides funds to telecommunications providers to subsidize service for low-income customers, high-cost areas, schools and libraries, and rural health care facilities. *Id.* ¶ 10. *See Rural Cellular Ass'n v. FCC*, 588 F.3d 1095, 1099 (D.C. Cir. 2009).

See 2019 NDAA, § 889(f)(3)(B). Thus, Congress defined "covered telecommunications equipment" under the 2019 NDAA to include video equipment produced by Hikvision or Dahua, if used for the listed purposes.

In November 2019, the FCC adopted its earlier-proposed rule prohibiting the use of Universal Service funds to purchase equipment or services from "a covered company posing a national security threat to the integrity of communications networks or the communications supply chain." *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, 34 FCC Rcd 11423, 11433, ¶ 26 (2019) (*Supply Chain Order*) (codified at 47 C.F.R. § 54.9). The FCC initially designated only Huawei and ZTE as "covered companies," but it set out procedures for designating additional companies. *Id.* The Fifth Circuit upheld the *Supply Chain Order*, finding that "[a]ssessing security risks to telecom networks falls in the FCC's wheelhouse," and that the FCC "reasonably acted within the broad authority Congress gave it to regulate communications." *Huawei Technologies*, 2 F.4th at 427.

3. Secure Networks Act

In March 2020, to further protect the nation's communications networks, Congress enacted the Secure and Trusted Communications Networks Act of 2019. Pub. L. No. 116-124, 134 Stat. 158 (2020) (codified as amended at 47 U.S.C. §§ 1601-1609) (Secure Networks Act). In brief, this law (1) requires the FCC to maintain a list of "covered communications equipment and services" that pose a national security risk, (2) prohibits the use of FCC-administered federal funds on covered equipment or services, and (3) establishes a reimbursement program for providers to replace covered equipment and services. *Id.* §§ 2–4.

Specifically, the FCC must place on the "Covered List" equipment that

> (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.

Secure Networks Act § 2(b)(1)–(2).

In determining whether equipment satisfies the first prong, the FCC must act "solely" based on one or more determinations from only four sources. *Id.* § 2(c). Three of those sources are identified groups of executive authorities: "any executive branch interagency body with appropriate national security expertise," the Department of Commerce, or "an appropriate national security agency." *Id.* § 2(c)(1),(2), (4). The fourth source is the 2019 NDAA: The Commission "shall place" on the Covered List whatever is "covered telecommunications equipment…, as defined" under section 889(f)(3) of the 2019 NDAA. *Id.* § 2(c)(3). Again, the 2019 NDAA refers to equipment from Dahua and Hikvision.

4. *Supply Chain Second Order*

On December 10, 2020, the FCC issued an order to implement the Secure Networks Act. *See Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, 35 FCC Rcd 14284 (2020) (*Supply Chain Second Order*). Under the Secure Networks Act, the agency observed, "where there is a determination from

one of [the enumerated] sources" that equipment poses a risk, the FCC "must" add that equipment to the Covered List. *Id.* ¶ 59.

In establishing procedures and criteria to guide the publication of the Covered List, the agency stated that the List would include video surveillance and telecommunications equipment produced by Hytera, Hikvision, and Dahua, with two qualifications. First, the FCC specified that such equipment would be on the Covered List only "to the extent it is used for public safety or security." *Id.* ¶ 68. Second, as required by the Secure Networks Act, the Commission provided that covered equipment must be "capable of the functions outlined in sections 2(b)(2)(A), (B), or (C) of the Secure Networks Act," *id.*—that is, routing or directing network traffic in certain ways, causing remote disruption of advanced communications, or "otherwise posing an unacceptable risk to the national security of the United States or the security and safety of United States persons." Secure Networks Act § 2(b)(2)(C). The agency found that where "an enumerated source ha[d] already performed" the analysis to find that "specific pieces of equipment or services belong[ed] on the Covered List," the agency would accept that assessment as a determination that the equipment also "otherwise pos[ed] an

unacceptable risk" to national security, within the meaning of section 2(b)(2)(C). *Supply Chain Second Order* ¶¶ 80–81.

On March 12, 2021, the FCC's Public Safety and Homeland Security Bureau published the Covered List of services and equipment deemed by the Commission to pose an unacceptable risk to national security. *Public Safety and Homeland Security Bureau Announces Publication of the List of Equipment and Services Covered by Section 2 of the Secure Networks Act*, 36 FCC Rcd 5534 (2021) (*2021 Covered List Public Notice*). As contemplated by the FCC's *Supply Chain Second Order*, this included video surveillance and telecommunications equipment produced by Hikvision and Dahua "to the extent it is used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes." *Id.*

No party petitioned for judicial or administrative review of either the FCC's *Supply Chain Second Order* or the Bureau's *2021 Covered List Public Notice*.

B. The FCC's Equipment Authorization Program

Under section 302 of the Communications Act, the FCC may, "consistent with the public interest, convenience, and necessity, make

reasonable regulations…governing the interference potential of devices" capable of emitting radio frequency emissions "in sufficient degree to cause harmful interference to radio communications." 47 U.S.C. § 302a(a);[2] *see also id.*§ 303(e) (agency "shall" as "public convenience requires" "regulate the kind of [radio] apparatus to be used with respect to its external effects"). Companies may not manufacture, import, or sell devices that do not comply with these regulations. *Id.* § 302a(b). Thus, "as a general matter, for [a radio frequency] device to be marketed or operated in the United States, it must have been authorized for use by the Commission." *Order* ¶ 25 (JA__). The FCC's regulations under section 302, known as its "equipment authorization" program, are codified at part 2 of its rules and "play a critical role in enabling the Commission to carry out its responsibilities under the Communications Act." *Order* ¶ 25 (JA__); *see* 47 C.F.R. §§ 2.801 *et seq.*, 2.901 *et seq.*, 2.1201 *et seq*. *See generally* 47 C.F.R. § 2.901 (FCC has developed requirements "[i]n order to carry out its responsibilities under the Communications Act and the various treaties and international regulations, and in order to promote efficient use of the radio spectrum").

[2] Section 302 of the Communications Act is codified at 47 U.S.C. § 302a because a former section 302 of the U.S. Code was repealed.

C. The Notice of Proposed Rulemaking

On June 17, 2021, the FCC issued a Notice of Proposed Rulemaking proposing to revise its equipment authorization rules to prohibit authorization of "covered" equipment on the Commission's Covered List. *See Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program*, ET Docket No. 21–232, 36 FCC Rcd 10578, 10596 ¶ 40 (2021) (*NPRM*) (JA__). The Commission's proposal differed from its earlier "covered equipment" measures, which concerned expenditure of USF funds, because it focused on authorization under its equipment authorization program, effectively banning the importation, sale, and marketing of covered equipment that had not yet been authorized.

The FCC explained that its proposed measures would serve the public interest by addressing significant national security risks, consistent with the Commission's statutory duty to safeguard "the national defense" and "promot[e] safety of life and property." *Id.* ¶ 65 (JA__) (citing 47 U.S.C. § 151). The agency also tentatively concluded that it had the authority to prohibit authorization of equipment on the Covered List, including under section 302 and under the Communications Assistance for Law Enforcement Act (CALEA), which

requires telecommunications carriers to ensure that the surveillance capabilities built into their networks can only be activated lawfully. *See id.* ¶¶ 66–68 (JA__). In further support for its proposal, the Commission referred to its ancillary authority under section 4(i) of the Act to enact such rules "as may be necessary in the execution of [the agency's] functions." *Id.* ¶ 65 (JA__) (citing 47 U.S.C. § 154(i)); *see id.* ¶ 69 (JA __).

D. Secure Equipment Act

On November 11, 2021, while the Commission's rulemaking was ongoing, Congress enacted the Secure Equipment Act of 2021, Pub. L. No. 117-55, 135 Stat. 423 (2021) (codified at 47 U.S.C. § 1601 note) (Secure Equipment Act). Congress required the FCC, within one year of the statute's enactment, to adopt rules in its ongoing proceeding, which Congress identified specifically by referencing the *NPRM* and the FCC docket number. *Id.* § 2(a)(1).[3]

The Secure Equipment Act goes on to provide:

---

[3] The law states: "Not later than 1 year after the date of the enactment of this Act, the Commission shall adopt rules in the proceeding initiated in the Notice of Proposed Rulemaking in the matter of Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program (ET Docket No. 21–232; FCC 21–73; adopted June 17, 2021), in accordance with paragraph (2), to update the equipment authorization procedures of the Commission." *Id.* §2(a)(1).

> In the rules adopted under paragraph 1, the Commission shall clarify that [it] will no longer review or approve any application for equipment authorization for equipment that is on the list of covered communications equipment or services published by the Commission under section 2(a) of the [Secure Networks Act].

Id. § 2(a)(2). The Act's legislative history reflects that Congress intended for the agency's implementing rule to cover equipment from Hikvision and Dahua. *See* Memorandum from House Committee on Energy and Commerce Staff, re *Full Committee Markup of 16 Health Bills and 8 Communications and Technology Bills* at 7 (July 19, 2021), *see* App. A.

E. *Order* on Review

On November 25, 2022, the FCC issued the *Order* on review "to further secure our communications networks and supply chains from equipment that poses an unacceptable risk to national security." *Order* ¶ 1 (JA__). As proposed in the *NPRM,* the agency amended its equipment authorization program to prohibit future authorization of equipment listed on the Commission's Covered List, published and maintained pursuant to the Secure Networks Act. *Id.* The agency left for another day, however, the question whether to "review or [revoke]…any…existing equipment authorization[s] granted prior to adoption of [the *Order*]." *Order* ¶ 107 (JA__).

1. Legal Authority

The FCC concluded that it had legal authority to prohibit the authorization of Covered Equipment both under the Secure Equipment Act and, independently, under earlier-enacted statutes. *Id.* ¶ 34–43 (JA__).

The agency first explained that, in providing that the FCC "shall adopt rules" and "shall clarify that [it] will no longer" authorize equipment on the Covered List, Secure Equipment Act §§ 2(a)(1)–(2), the Secure Equipment Act gave the FCC "express authority to adopt" the *Order*. *Id.* ¶ 39 (JA__).

Second, the FCC found that its pre-existing statutory authority provided an independently sufficient basis for its action. For one thing, the Commission explained, the grant of authority in section 302 to make rules "consistent with the public interest, convenience, and necessity" "governing the interference potential of devices which…are capable" of causing harmful interference gave it the power to address the interference potential of devices in accordance with the agency's other statutory responsibilities. *Id.* ¶ 40 (JA __). In particular, the agency observed, the phrase "the public interest" "provides independent authority to take into account" the national defense and the promotion of

safety of life and property—purposes for which the FCC was founded. *Id.* (citing 47 U.S.C. § 151). In addition, the Commission drew support for its rule from section 105 of CALEA, which requires telecommunications carriers to ensure that the surveillance capabilities built into their networks "can be activated only in accordance with a court order or other lawful authorization," and which requires the agency to issue implementing rules. *Id.* ¶ 41 (JA__) (citing 47 U.S.C. § 1004). The agency concluded that the *Order* "will help ensure that equipment that carriers include in their networks will not include such unlawful interception capabilities" because covered equipment "is far more likely to be subject to unauthorized access." *Id.*

2. Confirmation of the *Supply Chain Second Order* Interpretations of Covered List

In the *Order*, the FCC also offered "clarity" concerning "what constitutes 'covered equipment'" under the new rules. *Order* ¶ 120 (JA__). The agency summarized at length the provisions of the Secure Networks Act and its *Supply Chain Second Order*. For example, the FCC explained that the statute defined covered equipment based on any of four enumerated sources, including the 2019 NDAA, which in turn defined "covered telecommunications equipment" to include "video surveillance

and telecommunications equipment produced by Hytera, Hikvision, and Dahua (and their subsidiaries and affiliates) '[f]or the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes.'" *Id.* ¶ 130 (JA__) (quoting 2019 NDAA § 889).

The agency rejected arguments in comments submitted by Hikvision and Dahua that their equipment "cannot constitute covered communications equipment under the Secure Networks Act and section 889(f)(3) of the 2019 NDAA, and that it does not belong [on] the Commission's Covered List." *Id.* ¶ 166 (JA__); *see generally id.* ¶¶ 147–181 (JA__–__). The Commission explained that, in the 2019 NDAA, Congress prohibited procurement of the companies' video surveillance equipment, "because such equipment can pose an unacceptable risk to national security." *Id.* ¶ 168 (JA__). Because the Secure Networks Act in turn referenced that determination, the agency found it was "not in position to question that or not include [the companies' equipment] on the Covered List." *Id.*

The agency also found that, through the Secure Equipment Act—which was enacted after equipment from Dahua and Hikvision was already on the Covered List—"Congress…intended…to include the

telecommunications equipment and the video surveillance equipment that already was on the Covered List." *Id.* The agency also noted evidence that petitioners' video surveillance equipment "includes vulnerabilities that would allow hackers to access camera feeds and recordings, switch devices on and off, reposition cameras, hack into the networks in which they are connected, or use the devices in a botnet attack." *Order* ¶ 156 (JA__).

The agency disagreed with the companies' assertions that their video surveillance equipment "does not meet the 'capability' requirements under section 2(b) of the Secure Networks Act either with respect to being capable of routing or redirecting user data traffic or permitting visibility into any user data or packets or causing the network to be disrupted remotely." *Id.* ¶ 169 (JA__). The FCC observed, as it had already concluded in the *Supply Chain Second Order*, that Congress, through the 2019 NDAA, had "in effect…made th[e § 2(b)] capability determination…insofar as Congress has determined that it is capable of 'otherwise posing an unacceptable risk" to national security.'" *Id.*

The agency also rejected arguments that video surveillance equipment is not "communications equipment" or "essential to the provision of advanced communications service," as defined in section 9(4)

of the Secure Networks Act. *Order* ¶ 170 (JA__). The agency explained that, in the *Supply Chain Second Order*, it had already determined that the term "communications equipment or service" "means any equipment or service used in fixed and mobile networks that provides advanced communications service, provided the equipment or service includes or uses electronic components." *Id.* (quoting *Supply Chain Second Order* ¶ 52; 47 C.F.R. § 1.50001(c)). The FCC found that, in the 2019 NDAA, "Congress intended to capture…video surveillance equipment as 'covered' equipment, even if [it] is not core network equipment since the equipment is used (and indeed required) in the provision of a certain type of advanced communications service, i.e., video surveillance services." *Id.*

3. Scope of Rule

Because the Covered List covers video surveillance and telecommunications equipment from Hytera, Hikvision, and Dahua used "[f]or the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes," *Supply Chain Second Order* ¶ 68, the Commission prohibited the marketing and sale of this equipment for those same purposes. *Order* ¶ 177 (JA__).

Although the companies contended that their equipment was "not marketed or promoted for these prohibited purposes," a report in the record "found that between 2015 and 2021 nearly 1,700 state and local governments had purchased equipment on the Covered List, including equipment produced by Hytera, Hikvision, and Dahua." *Id.* ¶ 179 (JA__). And because the products are sold in the United States through independent dealers, the FCC observed that the companies "lack… oversight…over the marketing, distribution, and sales of their respective equipment." *Id.* ¶ 180 (JA__). The Commission was "not confident that, absent additional prescriptive measures and Commission oversight, Hytera, Hikvision, and Dahua 'telecommunications equipment' or 'video surveillance equipment' [would] not be marketed and sold for…purposes…prohibited under…the 2019 NDAA." *Id.* The *Order* therefore required that, before the FCC authorizes equipment from these companies, they "must each seek and obtain Commission approval for [their] respective plan[s] that will ensure that such equipment will not be marketed or sold" for the prohibited purposes. *Id.*

Because applicants for equipment authorization are now required to attest that their equipment is not "covered," the *Order* also provided "additional clarity on what constitutes 'covered' equipment that will be

prohibited.'" *Id.* ¶ 189 (JA__). In particular, because the Covered List reaches petitioners' equipment only when "used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes,"*2021 Covered List Public Notice* App., the agency further construed those elements, *see Order* ¶¶ 208–215 (JA__–__). The FCC explained that it would "interpret the scope of this section 889(f)(3)(B) prohibition broadly given the importance of preventing 'covered' equipment from being made available for prohibited uses that would pose an unacceptable risk to national security or the security of U.S. persons." *Id.* ¶ 208 (JA__). It explained:

> With regard to scope of "critical infrastructure" and the prohibition that we are adopting in this proceeding, we apply the meaning provided in section 1016(e) of the USA Patriot Act of 2001, namely, "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

Id. ¶ 212 (JA__). The agency also cited two lists of critical infrastructure from executive branch sources expert in national security: Presidential

Policy Directive 21, which cites sixteen critical infrastructure sectors,[4] and the list published by the National Risk Management Center subdivision of the Department of Homeland Security, which lists a set of 55 National Critical Functions to guide national risk management efforts. *Id.*[5] The agency found "that any systems or assets, physical or virtual, connected to the sixteen critical infrastructure sectors identified in [Presidential Policy Directive 21] or the 55 [national critical functions] identified in [the National Risk Management Center publication] could reasonably be considered 'critical infrastructure.'" *Id.*

The Commission delegated authority to two subdivisions "to develop further clarifications to inform applicants for equipment authorization" about what equipment is covered, and authorized those

---

[4] The sixteen sectors are chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, health care and public health, information technology, nuclear reactors/materials/waste, transportation systems, and water/waste water systems. 1 Pub. Papers 106, 114–115 (Feb. 12, 2013) (*Presidential Policy Directive 21*). *Available at* https://perma.cc/C6XA-D9Y5.

[5] National Risk Management Center, Cybersecurity and Infrastructure Security Agency, *National Critical Functions Status Update to the Critical Infrastructure Community* (2020) (*National Critical Functions Update*). *Available at* https://perma.cc/N3YB-LZC4.

subdivisions "to review efforts from and coordinate as necessary with [the FCC's] federal partners," including the Departments of Justice, Commerce, and Homeland Security, and the FBI. *Id.* ¶ 214 (JA__). The FCC also made clear that parties may bring requests for declaratory rulings "to clarify whether particular equipment is 'covered' for purposes of the equipment authorization prohibition." *Id.* ¶ 215 (JA__).

STANDARD OF REVIEW

Under the Administrative Procedure Act, a court may not overturn agency action unless it is arbitrary, capricious, or otherwise contrary to law. 5 U.S.C. § 706(2). "Under this 'deferential' standard, '[a] court simply ensures that the agency has acted within a zone of reasonableness and, in particular, has reasonably considered the relevant issues and reasonably explained the decision." *China Telecom*, 57 F.4th at 264–65 (quoting *FCC v. Prometheus Radio Project*, 141 S. Ct. 1150 (2021)). Courts must "presume the validity of agency action and must affirm unless the Commission failed to consider relevant factors or made a clear error in judgment." *Id.* (cleaned up). And a reviewing court must "accept the Commission's findings of fact so long as they are supported by substantial evidence on the record as a whole." *Id.* (cleaned up).

SUMMARY OF THE ARGUMENT

I.A. The FCC acted pursuant to an express direction in the Secure Equipment Act to change its rules to prohibit authorization of the equipment on the Covered List, which included video surveillance equipment produced by petitioners Dahua and Hikvision "for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes." 2019 NDAA § 889(f)(3)(B). In the *NPRM*, the FCC proposed to amend its rules to no longer authorize equipment on the Covered List to be sold or marketed in the United States. In the Secure Equipment Act, Congress directed the agency to do precisely what it had proposed in that proceeding. The agency was thus authorized—indeed was required—to prohibit the marketing or sale of equipment manufactured by Hikvision and Dahua for the listed purposes.

I.B. The Secure Equipment Act also confirms that the FCC already had sufficient authority to the take the actions it did in the *Order*. As the agency explained, section 302 of the Communications Act directs the agency to make rules "consistent with the public interest" to govern the interference potential of radio frequency devices. 47 U.S.C. § 302a(a); *see also id.* § 303(e). The *Order* amends the agency's rules made pursuant to

this provision, and the new rules serve the public interest because they are "essential to the national defense and to the promotion of public safety," *Order* ¶ 40 (JA__), purposes for which the agency was created, 47 U.S.C. § 151. Separately, the rules are authorized by the Communications Assistance for Law Enforcement Act, which tasks the agency with implementing a requirement that telecommunications providers ensure that communications are not intercepted unlawfully. 47 U.S.C. § 229(a)–(b), 1004. The FCC set out these interpretations of its authority in the *NPRM*, and Congress then passed the Secure Equipment Act, specifically directing the agency to act.

II.A. Most of petitioners' brief does not challenge the *Order* itself, but instead the agency's earlier implementation of the Secure Networks Act in the *Supply Chain Second Order*. But petitioners are well past the 60-day time limit set forth in the Hobbs Administrative Orders Review Act, 28 U.S.C. § 2344, to contest that (now two-year-old) order. Their challenge is well out of time.

Petitioners' challenge to the Commission's implementation of the Secure Networks Act is also foreclosed by the subsequent Secure Equipment Act. Congress was aware that petitioners' products were on the Covered List—as evidenced by its direct reference to the *NPRM* in

the Secure Equipment Act. That law's legislative history also mentions Hikvision and Dahua by name. Congress then ordered the agency to prohibit authorization of equipment on the Covered List. Petitioners' arguments that the FCC has misread the Secure Networks Act thus are badly misplaced.

IIB. Petitioners' arguments are meritless in any event. Petitioners argue that their equipment is not "communications equipment" under the Secure Networks Act because it is not "essential" to the provision of advanced communications service. Br. 28 (quoting Secure Networks Act § 9(4)). But, as the agency explained, "communications equipment" includes equipment used in video communications via broadband, which petitioners' products enable. *Order* ¶ 170 (JA__). The Secure Networks Act also refers to "communications equipment or service being covered telecommunications equipment or services, as defined in" the 2019 NDAA, which mentions Dahua and Hikvision video surveillance equipment specifically. *Id.* ¶ 168 (JA__) (quoting Secure Networks Act § 2(c)(4)).

IIC. Petitioners also argue that their products do not have the capability required by section 2(b)(2) of the Secure Networks Act. But the FCC explained that those products have the capability of "otherwise

posing an unacceptable risk" to national security under that section. *Order* ¶ 169 (JA__) (citing *Supply Chain Second Order* ¶¶ 80–81, 85). As the agency had previously found, where Congress or an agency had made a "specific," "granular" decision that products pose a threat, this prong of the test is satisfied. *Supply Chain Second Order* ¶ 80. Section 2(b)(2) serves as a separate check where the agency relies on a more general determination that a company is a threat, by focusing further on which equipment is dangerous. But here, the 2019 NDAA evidenced Congress's determination that petitioners' products were capable of posing a threat. *Id.* ¶¶ 80–82. That determination makes sense, because petitioners' products can form a part of an advanced communications network. *Order* ¶ 179 (JA__).

II.D. Finally, the FCC's guidance on the meaning of "critical infrastructure" was reasonable. Under the new rules, petitioners' products will not be prohibited entirely. Instead, those products cannot be marketed "for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes." The FCC adopted the definition of "critical infrastructure" from the USA Patriot Act as "systems and assets…so vital that [their] incapacity or destruction…would have a

debilitating impact" on national security, economic security, or public health and safety. *Order* ¶ 212 (JA__). The agency also relied on categories of assets identified in a presidential policy directive and a Department of Homeland Security publication. *Id.* Petitioners argue that the Commission's reading is overbroad and could reach surveillance of virtually all sectors of the economy, including "laundromats," and "used car lots." But those examples appear nowhere in the *Order* and do not reasonably fit into the Commission's description of critical infrastructure. Moreover, the agency invited parties to seek further clarification of specific examples by submitting a request for a declaratory ruling. Petitioners have not done so, and their unsupported conjecture is no basis to overturn the agency's reasonable action.

ARGUMENT

I. THE FCC ACTED WITHIN ITS AUTHORITY AND PURSUANT TO CONGRESS'S INSTRUCTION IN FORBIDDING AUTHORIZATION FOR COVERED EQUIPMENT.

In the Secure Equipment Act, Congress directed the FCC to amend its equipment authorization rules to clarify that the agency would no longer authorize equipment on the Covered List, precisely as the Commission had proposed in the *NPRM*. Secure Equipment Act § 2(a). The Secure Equipment Act thus either granted the FCC authority to

prohibit the marketing or sale of equipment on the Covered List, or confirmed the FCC's understanding that the agency had preexisting authority to do so, or both. Under any of these understandings, the agency was authorized to issue the *Order*.

A. The Secure Equipment Act Granted Authority for the *Order*.

In the *Order*, the agency was carrying out explicit instructions from Congress in the Secure Equipment Act. In the *NPRM*, the FCC proposed "revisions to the Commission's equipment authorization rules and processes to prohibit authorization of any 'covered' equipment on the Covered List." *NPRM* ¶ 40 (JA__). The agency explained that the "prohibition would apply to 'covered' equipment on the Covered List maintained and updated by" the Public Safety and Homeland Security Bureau—i.e., the Covered List required by the Secure Networks Act. *Id.*

While this rulemaking was pending, Congress passed the Secure Equipment Act, directing that the FCC within one year "shall adopt rules" in the proceeding initiated by the *NPRM*, referencing the proceeding by name and docket number. Secure Equipment Act § 2(a)(1). In the same statute, Congress directed the Commission to "clarify that [it] will no longer review or approve any application for equipment

authorization for equipment that is on the list of covered communications equipment or services published by the Commission under section 2(a) of the" Secure Networks Act. *Id.* §2(a)(2). In so doing, Congress expressly directed the FCC to take the actions in the *Order*, thereby authorizing—indeed requiring—the actions on review here. *See Order* ¶ 39 (JA__) ("the Commission is acting based on the clear and express statutory language contained in section 2(a)(1) of the Secure Equipment Act"); *id.* ¶ 168 (JA__) (in the Secure Equipment Act, "Congress expressly mandated that the Commission prohibit authorization of equipment on the Covered List as it had proposed to do in the *NPRM*").

B. Alternately, the FCC Already Had Authority for the *Order*, as Confirmed by the Secure Equipment Act.

Because the FCC's authority under the Secure Equipment Act is sufficient to sustain the *Order*, there is no reason for this Court to reach petitioners' contention that the Commission could not pass the rules under section 302 (Br. 40–46). But in any event, the FCC had authority to adopt the rules under section 302 of the Communications Act, as well as under the Communications Assistance for Law Enforcement Act. *See Order* ¶¶ 40–42 (JA__–__).

Section 302 of the Communications Act directs the FCC, "consistent with the public interest, convenience, and necessity," to "make reasonable regulations…governing the interference potential of devices which in their operation are capable of emitting radio frequency energy by radiation, conduction, or other means in sufficient degree to cause harmful interference to radio communications." 47 U.S.C. § 302a(a). *See also* 47 U.S.C. § 303(e) (authorizing the Commission to regulate a radio apparatus "with respect to its external effects"). The *Order* concerns the FCC's equipment authorization rules, which are indeed rules "governing the interference potential of devices…capable of…caus[ing] harmful interference to radio communications," as described by section 302. And the new rules serve to promote the "public interest" because, the agency found, "prohibiting authorization of equipment that has been placed on the Covered List is essential to the national defense and to the promotion of public safety." *Order* ¶ 40 (JA__). The FCC was created "for the purpose of the national defense [and] for the purpose of promoting safety of life and property." 47 U.S.C. § 151. It was therefore reasonable for the agency to interpret the promotion of the "public interest" under section 302 to encompass authority to prohibit devices and uses that might compromise

the security of the U.S. communications system. *See Huawei Technologies*, 2 F.4th at 427.

Petitioners argue that section 302 gives the FCC only the power to "govern interference potential" and to "establish minimum performance standards." Br. 42. But the statute directs the agency to ensure that its rules governing the interference potential of devices that emit radiofrequency energy are "consistent with the public interest, convenience and necessity." 47 U.S.C. § 302a(a). As the Supreme Court has explained, that public interest authority "is to be interpreted by its context, by the nature of radio transmission and reception, [and] by the scope, character, and quality of services." *NBC v. United States*, 319 U.S. 190, 216 (1943) (cleaned up). Here, the context is whether section 302 permits the Federal Communications Commission to forbid the import, marketing, and sale of radio frequency devices that Congress and other executive agencies have found threaten the integrity of the nation's communications network. Given the agency's explicit purpose to safeguard national security, the agency's interpretation of section 302 to encompass the regulation of radio frequency devices that could threaten the security of communications networks was reasonable. *See China Telecom*, 57 F.3d at 276 (citing *Haig v. Agee*, 453 U.S. 280, 292 (1981))

("Matters intimately related to foreign policy and national security are rarely proper subjects for judicial intervention.").

Separately, the Communications Assistance for Law Enforcement Act (CALEA) affords the FCC authority to issue the Order. *See Order* ¶ 41 (JA__); Pub. L. No. 103–414, 108 Stat. 4279 (1994) (codified at 47 U.S.C. § 1001 et seq.). This law requires telecommunications carriers to:

> 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.

47 U.S.C. § 1004. CALEA also requires the FCC to prescribe implementing rules "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).

In the *Order*, the Commission found that prohibiting the authorization of covered equipment "will help ensure that equipment that carriers include in their networks will not include such unlawful interception capabilities" because such covered equipment "is far more likely to be subject to unauthorized access." *Order* ¶ 41 (JA__); *see id.* ¶ 206 (JA__) (recognizing that petitioners' "devices are capable of storing

and sharing their content over broadband networks and thus being connect[ed] to the network,…become part of the network"). It was therefore reasonable for the FCC to take action to further prohibit unauthorized access as required by CALEA.[6]

If the Secure Equipment Act is not read as separately granting sufficient authority to issue the *Order*, it at a minimum served to confirm the FCC's understanding that it had preexisting authority to issue the *Order*. The FCC had explained its understanding that these statutes authorized these actions in the *NPRM*. *NPRM* ¶¶ 65–69 (JA__–__). Then Congress in the Secure Equipment Act referred to that *NPRM* and directed the FCC to "clarify" that it would no longer review or approve any application for equipment that is on the Covered List. Secure Equipment Act § 2(a). As the Commission explained, Congress thereby "clearly intended to ratify the Commission's tentative conclusions in the *NPRM* that it had authority as discussed therein." *Order* ¶ 42 (JA__).

---

[6] Petitioners do not challenge the agency's reading of CALEA in their opening brief. The Court may thus sustain the Commission's view of its authority on that basis alone. *See Maine Lobstermen's Ass'n v. Nat'l Marine Fisheries Serv.*, 70 F.4th 582, 594 (D.C. Cir. 2023) (arguments not raised in opening brief are waived).

II. THE FCC'S INTERPRETATION OF COVERED EQUIPMENT TO INCLUDE PETITIONERS' PRODUCTS FOR CERTAIN USES WAS REASONABLE AND APPROVED BY CONGRESS.

A. Most of Petitioners' Arguments About the Secure Networks Act Are Both Untimely and Foreclosed by the Secure Equipment Act.

Much of petitioners' brief does not challenge the *Order* itself, which declared that equipment on the Covered List would no longer be authorized. Petitioners instead largely argue that their equipment should not be on the Covered List to begin with. But the FCC placed petitioners' equipment on the Covered List years ago, in the March 2021 public notice issued pursuant to the December 2020 *Supply Chain Second Order*, where the Commission adopted its governing interpretations of the Secure Networks Act. *See Supply Chain Second Order* ¶ 68. The time for petitioners to have challenged those FCC actions is long past. Under the Hobbs Act, 28 U.S.C. § 2344, parties must petition for review within 60 days of agency action, and this Court lacks jurisdiction to hear later challenges. *See Bhd. of Locomotive Engineers & Trainmen v. Fed. R.R. Admin.*, 972 F.3d 83, 103 (D.C. Cir. 2020).

Courts recognize an exception to this jurisdictional limit where an agency "reopens" a previous decision by reconsidering it. *See Pub. Emps. for Env't Responsibility v. EPA*, -- F.4th --, 2023 WL 4714021 *6 (D.C. Cir.

July 25, 2023) ("*PEER*"). However, "[w]hen the agency merely responds to an unsolicited comment by reaffirming its prior position, that response does not create a new opportunity for review." *Id.* at *8 (cleaned up). *See also Sierra Club v. EPA*, 925 F.3d 490, 494 (D.C. Cir. 2019) (a petitioner "cannot comment on matters other than those actually at issue, goad an agency into a reply, and then sue on the grounds that the agency had re-opened the issue" (cleaned up)). Instead courts find reopening only where "the entire context of the proceeding, includ[ing] all relevant proposals and reactions of the agency," indicate "that the agency has undertaken a serious, substantive reconsideration of the existing rule." *PEER*, 2023 WL 4714021 at *6 (cleaned up). Petitioners bear the burden of showing reopening has occurred. *Id.*

Here, the FCC's *Order* shows none of the hallmarks of reopening. In the underlying *NPRM*, the Commission nowhere signaled that it intended to reexamine its interpretation of the Secure Networks Act as set out in the *Supply Chain Second Order*. Instead, the *NPRM* described the previous order in some detail and then proposed new rules to "build[] on [those] actions." *NPRM* ¶¶ 15–17, 22, 35–37 (JA__, __–__, __–__). Nothing in the *NPRM* invited comment on whether the agency should interpret the Secure Networks Act differently.

Likewise, in the *Order* on review, the FCC described what equipment was already on the Covered List, and described its previous interpretations of the Secure Networks Act. *Order* ¶¶ 147–152 (JA__). In response to petitioners' arguments that their equipment does not "belong[] on the Covered List," the agency "explain[ed] that their 'telecommunications equipment' and 'video surveillance equipment' was previously determined to be 'covered' and has accordingly been placed on the Covered List." *Id.* ¶ 157 (JA__). The agency also specifically found it had already decided the issues petitioners raise here regarding the scope of "communications equipment" and "capability" under the Secure Networks Act. *See Order* ¶ 170 (JA__) (agency had "already interpreted 'communications equipment or service' and what is 'essential,'" in the *Supply Chain Second Order*); *id.* ¶ 169 (JA__) (agency had "already concluded" in the *Supply Chain Second Order* that Congress had "in effect…made [the] capability determination" required by section 2(b)(2)(C)).

To be sure, the agency offered new, additional guidance about what it means for equipment to be used "for the purpose…physical security surveillance of critical infrastructure…." *Id.* ¶¶ 189–215 (JA__). Petitioners' challenge to the agency's additional guidance on what

constitutes "critical infrastructure" is therefore timely. *See infra* II.D. However, in challenging the FCC's interpretation of what constitutes equipment "essential to the provision of advanced services" and "capable of posing an unacceptable risk to national security," petitioners' rely on arguments concerning readings set out in the 2020 *Supply Chain Second Order*. *See infra* II.B–C. While petitioners remain free to raise those arguments before the Commission in a petition for a new rulemaking, 47 C.F.R. § 1.401—and would be free to seek judicial review of the FCC's resolution of any such petition—this Court may not reach those issues in this case, on review of a decision that did not reopen them.

Even if petitioners' challenge to the inclusion of their equipment on the Covered List were not untimely, their arguments concerning the meaning of the Secure Networks Act have been foreclosed by the Secure Equipment Act, which ratified the agency's Covered List. "Congress is presumed to be aware of an administrative or judicial interpretation of a statute and to adopt that interpretation when it re-enacts a statute without change." *Jackson v. Modly*, 949 F.3d 763, 773 (D.C. Cir. 2020) (quoting *Merrill Lynch, Pierce, Fenner & Smith, Inc. v. Curran*, 456 U.S. 353, 382 n.66 (1982)). "This indication is particularly strong if evidence exists of the Congress's awareness of and familiarity with such an

interpretation." *Id.* (citing *Bob Jones Univ. v. United States*, 461 U.S. 574, 599–602 (1983)).

Here, there is strong evidence that Congress was aware of the FCC's implementation of the Secure Networks Act. Congress passed the Secure Equipment Act after the FCC had issued the *NPRM* in this proceeding, where the agency (1) reiterated its understanding of the Secure Networks Act, as reflected in the definitions from the *Supply Chain Second Order*; (2) noted petitioners' equipment was on the Covered List; and (3) proposed to cease authorizing covered equipment. *NPRM* ¶¶ 15–17, 22, 35–37 (JA__–__, __, __–__). The Secure Equipment Act then directed the FCC to adopt rules clarifying it would no longer authorize "equipment that is on the list of covered communications equipment or services published by the Commission under section 2(a) of the [Secure Networks Act]." Secure Equipment Act § 2(a)(2).

Both at the time of the *NPRM* and when Congress enacted the Secure Equipment Act, petitioners' equipment was on the Covered List, based on the FCC's understanding of the Secure Networks Act. By directing the FCC to no longer authorize equipment on that list, Congress expressed a clear intention that the agency should no longer authorize

petitioners' covered equipment.[7] In the face of this ratification, there is no room for petitioners to challenge the Commission's earlier interpretation of the Secure Networks Act, which led to the inclusion of their equipment on the Covered List.

B. Video Surveillance Equipment Is Essential to the Provision of Advanced Services Within the Meaning of the Secure Networks Act.

Even if petitioners' arguments about the meaning of the Secure Networks Act were not untimely and foreclosed by the Secure Equipment Act, those arguments fail on the merits.

Petitioners first argue that their products are not "communications equipment" under the Secure Networks Act. Br. 28-31. That statute defines "communications equipment or service" as "any equipment or service that is essential to the provision of advanced communications service." Secure Networks Act § 9(4)–(5). "Advanced communications

---

[7] If further evidence were needed, the memorandum prepared by the House Committee on Energy and Commerce on mark-up of the Secure Equipment Act unequivocally states that the law "would prevent further integration and sales of Huawei, ZTE, Hytera, Hikvision, and Dahua—all Chinese state-backed or directed firms—in the United States regardless of whether federal funds are involved." Memorandum from House Committee on Energy and Commerce Staff, re *Full Committee Markup of 16 Health Bills and 8 Communications and Technology Bills* at 7 (July 19, 2021). *See* App. A.

service," in turn, "has the meaning given the term 'advanced telecommunications capability'" in section 706 of the Telecommunications Act of 1996"—that is, "high-speed, switched, broadband telecommunications capability that enables users to originate and receive high-quality voice, data, graphics, and video telecommunications using any technology." *Id.* § 9(1); 47 U.S.C. § 1302(d)(1).

In the *Supply Chain Second Order*, the FCC noted that the Secure Networks Act "does not define which factors make equipment or service 'essential'" to the provision of advanced communications service, and it then interpreted "communications equipment or service" to "include all equipment or services used in fixed and mobile broadband networks, provided they include or use electronic components." *Supply Chain Second Order* ¶¶ 51, 52. The Commission found that "all equipment or services that include or use electronic components can be reasonably considered essential to broadband networks," and further that this "definition will provide a bright-line rule that will ease regulatory compliance and administrability." *Id.* ¶ 52. The definition was "appropriately tailored" because "it provides clear and simple guidance

to regulated parties while still covering any equipment and service that could potentially pose a threat to national security." *Id.* ¶ 53.

Petitioners assert that their video cameras and recorders are not "indispensable to the provision of broadband service" (Br. 28), but the Secure Networks Act defines advanced communications service by reference to section 706 of the Telecommunications Act of 1996, which describes "broadband telecommunications capability that enables users to originate and receive high-quality …video telecommunications using any technology." 47 U.S.C. § 1302(d)(1). In other words, advanced telecommunications include video telecommunications, like the services enabled by petitioners' products. As the *Order* points out, petitioners' "equipment is used (and indeed required) in the provision of a certain type of advanced communications service, i.e., video surveillance services." *Order* ¶ 170 (JA__). So while petitioners' video cameras and recorders are not essential to every type of advanced telecommunications—for example they are not essential to the transmission of internet protocol information packets over the internet backbone—they are essential to certain types—namely, the transmission of video information over the internet for video surveillance. *See id.* (petitioners' equipment "can be interconnected [to a telecommunications

or broadband network], and often is"). They are thus "essential to the provision of advanced communications service," and so fall within the definition of "communications equipment" under the Secure Networks Act.

As the *Order* explains, while it is possible to operate petitioners' equipment without an internet connection, comments noted that "most video surveillance equipment today has internet connectivity as a widely-demanded feature," and "Hikvision surveillance cameras are generally marketed as Internet-protocol (IP) cameras that are designed and marketed for use connected to internet." *Order* ¶ 206 (JA__). More generally, the agency found that video surveillance equipment that "make[s] use of broadband capabilities, such as video recorders, video surveillance servers, and video surveillance data storage" can be connected to the network, and so "become part of the network." *Id.* ¶ 206 (JA__). This is a reasonable interpretation of the Secure Networks Act.[8]

---

[8] Petitioners allege that this reading of "communications equipment" is inconsistent with the FCC's *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs,* 36 FCC Rcd 11958 (2021) (*Supply Chain Third Order*), where the agency found that petitioners' products were not eligible for the "rip-and-replace" program that subsidizes small broadband providers to remove some covered equipment. Br. 29. But the *Supply Chain Third Order* simply recognized that another recent statute had allocated funding only to

The Commission's reading is bolstered by the Secure Networks Act's incorporation of determinations from the 2019 NDAA. *See id.* ¶ 170 (JA__). The Secure Networks Act directs the agency to identify covered communications equipment based in part on the definition set out in the 2019 NDAA, a definition that encompasses "video surveillance and telecommunications equipment produced by" Hytera, Hikvision, or Dahua. 2019 NDAA § 889 (f)(3)(B); *see* Secure Networks Act § 2(c)(3). Thus, the Secure Networks Act incorporates a definition of covered "communications equipment or service" from the 2019 NDAA that includes petitioners' video surveillance equipment.[9] It is therefore a reasonable inference that petitioners' video surveillance equipment is

---

replace Huawei and ZTE equipment. *Supply Chain Third Order* ¶ 22. The FCC found that the Covered List was unchanged and included equipment produced by Hikvision and Dahua. *Id.* ¶ 29 & n.90. The agency also reiterated that section 2(b)(2)(C) of the Secure Networks Act is "indicative of Congress's intent to encompass on the Covered List equipment and services beyond the narrower list of enumerated functions" in sections 2(b)(2)(A) & (B). *Id.* ¶ 30.

[9] Petitioners argue (Br. 30) that Congress showed an intention to exclude their products in the Secure Networks Act by using the term "communications equipment or services," as opposed to the term "telecommunications or video surveillance equipment" in the 2019 NDAA. They ignore that the Secure Networks Act explicitly incorporates the definition from the 2019 NDAA, and also that "advanced communications" is a broader term that already includes broadband video services. *Order* ¶ 170 (JA__).

part of the equipment that Congress intended to target with the Secure Networks Act.

C. Video Surveillance Equipment Is Capable of Posing an Unacceptable Risk to National Security Within the Meaning of the Secure Networks Act.

Equipment is covered under the Secure Networks Act if it satisfies two conditions. First, under section 2(b)(1), it must be "communications equipment…produced…by [an] entity" such that equipment from that entity "poses an unacceptable risk" to national security based on determinations by certain Executive Branch agencies or in the 2019 NDAA. Secure Networks Act § 2(b)(1). Second, under section 2(b)(2), the equipment must be "capable" of at least one of the following:

> (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.

Id. § 2(b)(2). In the *Supply Chain Second Order*, the FCC found that the last of these capabilities—posing an unacceptable risk to national security—will be satisfied where a determination for the first prong "indicates that a specific piece of equipment or service poses an

unacceptable risk" to national security. *Supply Chain Second Order* ¶ 80. In those circumstances, a determination satisfying the section 2(b)(1) requirement will also satisfy the section 2(b)(2) capability requirement.

As the FCC explained in the *Supply Chain Second Order*, this reading does not minimize the capability prong of the test or disregard sections 2(b)(2)(A) and (B), which refer to routing, redirecting, or disrupting traffic. *Id.* ¶ 81. "Those sections play an important role in determining which specific pieces of equipment or services belong on the Covered List when [the agency] receive[s] a more general determination." *Id.*; *see id.* ¶ 84 (a determination that "failed to indicate the source or type of communications equipment or service that the originating source found potentially insecure" would be insufficient). But "when a determination covers a specific piece of equipment…and the [expert] agency [or statute] has indicated that such equipment…poses a national security risk," the FCC is obligated to recognize that the equipment also has the "capability" to pose an unacceptable risk to national security, within the meaning of the Secure Networks Act. *Id.* ¶ 81; *see id.* ¶ 80 (Commission was "bound to accept" a "granular" national security determination about specific equipment).

Petitioners contend that the Commission failed to make a finding that their products have the capability required by section 2(b)(2). Br. 34. Not so. The agency found that Congress—by mentioning petitioners' equipment by name and type in the 2019 NDAA—"has already performed the analysis on whether the equipment" has the capability to pose an unacceptable threat to national security under section 2(b)(2)(C). *Order* ¶ 169 (JA__) (citing *Supply Chain Second Order* ¶¶ 80–81, 85).

Nor does the agency's interpretation read section 2(b)(2) out of the statute, as petitioners contend. Br. 34. Not every determination that satisfies section 2(b)(1) will satisfy section 2(b)(2). Where the agency relies on a "more general determination" that a particular company, for example, represents an unacceptable threat under section (2)(a), then the capability requirements in section 2(b) "play an important role in determining which specific pieces of equipment or services belong on the Covered List." *Supply Chain Second Order* ¶ 81. It is only where Congress (or another source) has already made a determination about "a specific piece of equipment," *id.*—such as listing petitioners' video surveillance equipment in the 2019 NDAA—that the same determination will satisfy both section 2(b)(1) and 2(b)(2)(C).

Petitioners also argue that because 2(b)(2)(A) and (B) refer to routing and redirecting user traffic and disrupting advanced communications networks, 2(b)(2)(C)'s reference to an unacceptable risk to national security "must be related to a device's ability to interact harmfully with a network." Br. 36. Even under this reading, petitioners' devices can be employed as part of a network-based video surveillance system—a form of advanced communications, *Order* ¶ 179 (JA__)—and if they are compromised, that would indeed constitute harmful interaction with a communications network. For example, comments from one technology security firm contended that video surveillance equipment "includes vulnerabilities that would allow hackers to access camera feeds and recordings, switch devices on and off, reposition cameras, hack into the networks in which they are connected, or use the devices in a botnet attack." *Id.* ¶ 156 (JA__).[10] It was reasonable for the

[10] *See generally, e.g.,* BBC Panorama, *The tech flaw that lets hackers control surveillance cameras*, BBC News, June 26, 2023 (*available at* https://perma.cc/6QPZ-QT5R) (discussing security flaws in Dahua and Hikvision cameras; "Security experts fear the cameras have the potential to be used as a Trojan horse to play havoc with computer networks…."); Brian Contos, *The Secret, Insecure Life of Security Cameras*, Forbes, Mar. 1, 2023 (*available at* https://perma.cc/B6GT-NJMR) (smart cameras often "fail at basic cybersecurity," making them "an advantageous asset for

Commission, as the agency tasked with administering the Secure Networks Act, to conclude that Congress viewed video surveillance equipment as capable of compromising national security within the meaning of the Secure Networks Act section 2(b)(2)(C). *See Supply Chain Second Order* ¶ 81 ("If the determination is specified to a particular piece of communications equipment or service, we have no discretion to exclude that determination from the Covered List.").[11]

D. The FCC's Interpretation of "Critical Infrastructure" Under the Statutes Is Reasonable.

Because applicants for equipment authorization must now attest that the equipment in question is not covered, the *Order* "provide[s] additional clarity on what constitutes 'covered' equipment that will be

---

hackers, from hijacking [the cameras'] services to stealing company data and spying on business operations").

[11] Petitioners argue (Br. 40) that the FCC cannot rely the 2019 NDAA because that law does not prohibit the expenditure of federal funds on equipment that "cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles." 2019 NDAA § 889(a)(2)(B) & (b)(3)(B). They assert that their equipment cannot permit visibility into user data, but offer no proof of this assertion—an assertion at odds with concerns expressed in the record. *Order* ¶ 156 (JA__). Moreover, the General Services Administration's procurement rules implementing the 2019 NDAA prohibit the purchase of video surveillance and telecommunications equipment from Dahua and Hikvision. *Id.* ¶ 151 (JA__).

prohibited, as several [commenters had] requested." *Order* ¶ 189 (JA __–__); *see id.* ¶¶ 189–215 (JA__–__). The Commission explained that equipment from Hytera, Hikvision, and Dahua is covered only "[f]or the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes," as set out in the 2019 NDAA. *Order* ¶ 176 (JA__). In order to implement this ban, the FCC (1) "will only conditionally authorize the marketing and sale of such equipment authorization subject to this prohibition," (2) "will require labeling requirements that prominently state this prohibition," and (3) will require each entity to have a plan to ensure that such equipment will be not be marketed or sold for the prohibited purpose, including measures to ensure compliance from distributors and dealers. *Id.* ¶¶ 177, 180 (JA__).

The *Order* also offered additional guidance on how the Commission interprets the restriction on use of the equipment "for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes." *See Order* ¶¶ 208–214 (JA__–__). The agency first made clear that it would construe the terms "broadly in order to prohibit authorization of equipment that poses an unacceptable risk to national

security of the United States or to the security or safety of U.S. persons." *Id.* ¶ 209 (JA__).

The agency interpreted "critical infrastructure" to have the meaning provided in section 1016(e) of the USA Patriot Act of 2001: "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." 42 U.S.C. § 5195(c)(e).

The agency also referred to two additional sources of guidance. First, it referenced Presidential Policy Directive 21, the *Directive on Critical Infrastructure Security and Resilience*, which "advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure" and identifies sixteen critical infrastructure sectors. *Order* ¶ 212 (JA__) (citing *Presidential Policy Directive 21* at 106, 114–115, see above at n.4). Second, the agency referenced a publication from the National Risk Management Center, a subdivision of the Department of Homeland Security, which lists 55 "National Critical Functions" to guide national risk management efforts. *Id.* (citing *National Critical Functions Update*, see above at n.5). The

agency noted that the National Risk Management publication defines "critical infrastructure" much like the definition in "the USA Patriot Act," namely "functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." *Id.* The agency stated that for the purposes of implementing its rules, "we find that any systems or assets, physical or virtual, connected to the sixteen critical infrastructure sectors identified in [Presidential Policy Directive 21] or the 55 [national critical functions] identified in [the National Risk Management Center publication] could reasonably be considered 'critical infrastructure.'" *Id.*

The FCC then delegated to two subdivisions the authority "to develop further clarifications to inform applicants for equipment authorization…with more specificity and detail" about what equipment is covered, and to coordinate with the FCC's "federal partners," including the Departments of Justice and Homeland Security, and the FBI. *Id.* ¶ 214. Finally, the FCC made clear that any party may bring a request for declaratory ruling "to clarify whether particular equipment is 'covered.'" *Id.* ¶ 215 (JA__).

In sum, the agency explicated the meaning of the term "critical infrastructure" by reference to a statute, a presidential directive, and an expert agency publication and invited parties to seek further clarification through declaratory ruling. This was a modest and reasonable approach. Parties had asked for further guidance on the meaning of the term, and the agency provided direction based on sources produced by experts in national security and critical infrastructure, in conjunction with a process for further clarification.

Petitioners argue that the Commission's measured reading was nevertheless improper and overbroad (Br. 50–58), and that it might go so far as to include any sector of the economy as "critical infrastructure," including "laundromats," and "used car lots" (Br. 50, 56).[12] But those examples appear nowhere in the *Order*. To be sure, Presidential Policy

[12] Petitioners argue that, because the 2019 NDAA applies to the government as a whole, the FCC's explication of the term "critical infrastructure" does not deserve deference under *Chevron U.S.A., Inc. v. Nat. Res. Def. Council, Inc.,* 467 U.S. 837 (1984). Br. 47–50. But while this term is incorporated from the 2019 NDAA, the agency interpreted its scope only for the purposes of its own rules—without purporting to say what the term means in other contexts, such as the 2019 NDAA procurement restrictions. *Chevron* deference is therefore appropriate. In any case, the agency's interpretation was appropriate under any standard of review.

Directive 21 and the National Risk Management Center publication refer to a wide variety of sectors, but the FCC referred to these against the background of adopting the USA Patriot Act definition of assets so vital that their loss would be debilitating to national security. *Order* ¶ 212 (JA__). And if there is indeed any doubt about whether petitioners' products can be marketed to laundromats, petitioners need only seek guidance from the Commission by submitting a request for a declaratory ruling. They have not done so, and their farfetched examples provide no basis on which to overturn the agency's reasonable action.

CONCLUSION

The petitions for review should be denied.

Dated: July 31, 2023

Respectfully submitted,

/s/ Matthew J. Dunne

Brian M. Boynton
Principal Deputy Assistant Attorney General

Sharon Swingle
Casen Ross
Attorneys

U.S. DEPARTMENT OF JUSTICE
CIVIL DIVISION
950 Pennsylvania Ave. NW
Washington, DC 20530

Counsel for Respondent United States of America[*]

P. Michele Ellison
General Counsel

Jacob M. Lewis
Deputy General Counsel

Sarah E. Citrin
Deputy Associate General Counsel

Matthew J. Dunne
Counsel

FEDERAL COMMUNICATIONS COMMISSION
45 L Street NE
Washington, DC 20554
(202) 418-1740
fcclitigation@fcc.gov

Counsel for Respondent Federal Communications Commission

[*] Filed with consent pursuant to D.C. Circuit Rule 32(a)(2).

CERTIFICATE OF COMPLIANCE

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) and D.C. Circuit Rule 32(e)(1):

   ☒ this document contains 11,237 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 for Office 365 in 14-point Century Schoolbook, *or*

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

/s/ Matthew J. Dunne
Matthew J. Dunne
Counsel for Respondents

APPENDIX

COMMITTEE ON
ENERGY & COMMERCE
CHAIRMAN FRANK PALLONE, JR.

MEMORANDUM

July 19, 2021

To: Committee on Energy and Commerce Members and Staff

Fr: Committee on Energy and Commerce Staff

Re: Full Committee Markup of 16 Health Bills and 8 Communications and Technology Bills

On **Wednesday, July 21, 2021, at 10 a.m. (EDT) in the John D. Dingell Room, 2123 of the Rayburn House Office Building, and via Cisco Webex online video Conferencing**, the Committee on Energy and Commerce will hold a markup of the following 24 bills:

H.R. 4369, the "National Centers of Excellence in Advanced and Continuous Pharmaceutical Manufacturing Act"; **H.R. 654**, the "Drug-Free Communities Pandemic Relief Act"; **H.R. 2051**, the "Methamphetamine Response Act of 2021"; **H.R. 2379**, the "State Opioid Response Grant Authorization Act of 2021"; **H.R. 2364**, the "Synthetic Opioid Danger Awareness Act"; **H.R. 2355**, the "Opioid Prescription Verification Act of 2021"; **H.R. 4026**, the "Social Determinants of Health Data Analysis Act of 2021"; **H.R. 3743**, the "Supporting the Foundation for the National Institutes of Health and the Reagan-Udall Foundation for the Food and Drug Administration Act"; **H.R. 550**, the "Immunization Infrastructure Modernization Act"; **H.R. 1550**, the "Promoting Resources to Expand Vaccination, Education and New Treatments for HPV Cancers Act of 2021" (the "PREVENT HPV Cancers Act of 2021"); **H.R. 951**, the "Maternal Vaccination Act"; **H.R. 4387**, the "Maternal Health Quality Improvement Act of 2021"; **H.R. 3742**, the "Vaccine Information for Nursing Facility Operators Act" (the "Vaccine INFO Act"); **H.R. 2347,** the "Strengthening the Vaccines for Children Act of 2021"; **H.R. 3894**, the "Collecting and Analyzing Resources Integral and Necessary for Guidance for Social Determinants Act of 2021" (the "CARING for Social Determinants Act of 2021"); **H.R. 4406**, the "Supporting Medicaid in the U.S. Territories Act"; **H.R. 2685,** the "Understanding Cybersecurity of Mobile Networks Act"; **H.R. 3919**, the "Secure Equipment Act of 2021"; **H.R. 4028**, the "Information and Communication Technology Strategy Act"; **H.R. 4032**, the "Open RAN Outreach Act"; **H.R. 4045**, the "Future Uses of Technology Upholding Reliable and Enhanced Networks Act" (the "FUTURE Networks" ACT); **H.R. 4046**, the "NTIA Policy and Cybersecurity Coordination Act"; **H.R. 4055**, the "American Cybersecurity Literacy Act"; and **H.R. 4067**, the "Communications Security Advisory Act of 2021".

I. H.R. 4369, THE "NATIONAL CENTERS OF EXCELLENCE IN ADVANCED AND CONTINUOUS PHARMACEUTICAL MANUFACTURING ACT"

H.R. 4369, the "National Centers of Excellence in Advanced and Continuous Pharmaceutical Manufacturing Act", introduced by Chairman Pallone (D-NJ) and Rep. Guthrie (R-KY), would amend the 21st Century Cures Act to direct the Food and Drug Administration (FDA) to designate National Centers of Excellence in Advanced and Continuous Pharmaceutical Manufacturing (NCEs). NCEs would work with FDA and industry to craft a national framework for advanced and continuous manufacturing implementation, including supporting additional research and development of this technology, workforce development, standardization, and collaborating with manufacturers to support adoption of advanced and continuous manufacturing. The bill authorizes $100 million to be appropriated for NCEs each year from fiscal year (FY) 2021 through FY 2025.

On July 15, 2021, the Subcommittee on Health favorably forwarded H.R. 4369, as amended, to the full Committee by a voice vote.

II. H.R. 654, THE "DRUG-FREE COMMUNITIES PANDEMIC RELIEF ACT"

H.R. 654, the "Drug-Free Communities Pandemic Relief Act", was introduced by Reps. Joyce (R-OH) and Kilmer (D-WA). This bill would allow the Drug-Free Communities program to waive a grantee's matching requirement during the COVID-19 pandemic if they are unable to meet the match. This bill also increases the administrative cap on the Drug-Free Communities program from eight percent to 12 percent.

On July 15, 2021, the Subcommittee on Health favorably forwarded H.R. 654, as amended, to the full Committee by a voice vote.

III. H.R. 2051, THE "METHAMPHETAMINE RESPONSE ACT OF 2021"

H.R. 2051, the "Methamphetamine Response Act of 2021", was introduced by Reps. Peters (D-CA) and Curtis (R-UT). This bill would designate methamphetamine as an emerging threat and requires the Office of National Drug Control Policy (ONDCP) to develop a national plan to prevent methamphetamine addiction from becoming a crisis.

On July 15, 2021, the Subcommittee on Health favorably forwarded H.R. 2051, without amendment, to the full Committee by a voice vote.

IV. H.R. 2379, THE "STATE OPIOID RESPONSE GRANT AUTHORIZATION ACT OF 2021"

H.R. 2379, the "State Opioid Response Grant Authorization Act of 2021", was introduced by Reps. Trone (D-MD) and Sherrill (D-NJ). This bill would authorize the State Opioid Response Grant program and would harmonize the uses of these grants with the opioid funding provided under the 21st Century Cures Act. This bill also requires the U.S. Government

Accountability Office (GAO) to assess how grant funding is allocated to States, State perspectives on funding levels, and how grant funding is awarded under similar programs.

On July 15, 2021, the Subcommittee on Health favorably forwarded H.R. 2379, as amended, to the full Committee by a voice vote.

V. H.R. 2364, THE "SYNTHETIC OPIOID DANGER AWARENESS ACT"

H.R. 2364, the "Synthetic Opioid Danger Awareness Act", was introduced by Reps. Kim (D-NJ) and Pappas (D-NH). This legislation requires the Centers for Disease Control and Prevention (CDC) to implement a public education campaign related to synthetic opioids, including fentanyl and its analogues. In addition, the National Institute for Occupational Safety and Health would be required to publish a training guide and webinar for first responders and other individuals related to exposures to synthetic opioids.

On July 15, 2021, the Subcommittee on Health favorably forwarded H.R. 2364, as amended, to the full Committee by a voice vote.

VI. H.R. 2355, THE "OPIOID PRESCRIPTION VERIFICATION ACT OF 2021"

H.R. 2355, the "Opioid Prescription Verification Act of 2021", was introduced by Reps. Davis (R-IL), Bilirakis (R-FL), and Wagner (R-MO). This bill directs federal agencies to develop, disseminate, and periodically update training materials for pharmacists on verifying the identity of the patient. It also creates a preference for grants awarded to states by CDC for evidence-based overdose prevention activities to states that utilize prescription drug monitoring programs (PDMPs), require prescribers of certain controlled substances to utilize electronic prescribing, and require entry of information about the purchase of such prescriptions into the State's PDMPs including the National Drug Code or compounded identifier, the quantity dispensed, the patient identifier, and the date filled.

On July 15, 2021, the Subcommittee on Health favorably forwarded H.R. 2355, as amended, to the full Committee by a voice vote.

VII. H.R. 4026, THE "SOCIAL DETERMINANTS OF HEALTH DATA ANALYSIS ACT OF 2021"

H.R. 4026, the "Social Determinants of Health Data Analysis Act of 2021", introduced by Reps. Burgess (R-TX) and Blunt Rochester (D-DE), requires the Comptroller General of the United States to submit to Congress within two years of enactment a report on the actions taken by the Secretary of Health and Human Services (HHS) to address social determinants of health. The report shall include: an analysis of how data collection undertaken by HHS complies with Federal and state privacy laws and regulations, a description of any coordination by HHS with other relevant Federal, State, and local agencies, an identification of any potential for duplication or any barriers, and recommendations on how to foster public-private partnerships and leverage the private sector to address social determinants of health.

On July 15, 2021, the Subcommittee on Health favorably forwarded H.R. 4026, without amendment, to the full Committee by a voice vote.

VIII. H.R. 3743, THE "SUPPORTING THE FOUNDATION FOR THE NATIONAL INSTITUTES OF HEALTH AND THE REAGAN-UDALL FOUNDATION FOR THE FOOD AND DRUG ADMINISTRATION ACT"

H.R. 3743, the "Supporting the Foundation for the National Institutes of Health and the Reagan-Udall Foundation for the Food and Drug Administration Act", introduced by Reps. Hudson (R-NC) and Eshoo (D-CA), would authorize the National Institutes of Health (NIH) and FDA to increase transfer authority for funding to their supporting foundations, the Foundation for the National Institutes of Health (FNIH) and the Reagan-Udall Foundation for the Food and Drug Administration.

On July 15, 2021, the Subcommittee on Health favorably forwarded H.R. 3743, without amendment, to the full Committee by a voice vote.

IX. H.R. 550, THE "IMMUNIZATION INFRASTRUCTURE MODERNIZATION ACT"

H.R. 550, the "Immunization Infrastructure Modernization Act", introduced by Reps. Kuster (D-NH) and Bucshon (R-IN), would authorize $400 million for grants to expand, enhance, and improve immunization information systems administered by health departments and used by health care providers. This bill directs HHS to develop a strategy to improve immunization information systems, designate data and technology standards for the systems, and award grants to health departments and government organizations to improve their immunization systems based on the developed standards. It also requires HHS to report to the Committee one year after enactment on the barriers to public health authorities on implementing interoperable immunization information systems, the exchange of information, or reporting, as well as the barriers to establish effective networks to support immunization reporting and monitoring and an assessment of immunization coverage and access including any disparities or gaps. This bill also requires CDC to provide technical assistance to health care providers and adds scheduling and administration of vaccinations as an allowable use of grant funds.

On July 15, 2021, the Subcommittee on Health favorably forwarded H.R. 550, as amended, to the full Committee by a voice vote.

X. H.R. 1550, THE "PROMOTING RESOURCES TO EXPAND VACCINATION, EDUCATION AND NEW TREATMENTS FOR HPV CANCERS ACT OF 2021" (THE "PREVENT HPV CANCERS ACT OF 2021")

H.R. 1550, the "PREVENT HPV Cancers Act of 2021", introduced by Reps. Castor (D-FL) and Schrier (D-WA), would promote public awareness of human papilloma virus (HPV) vaccines, which can prevent HPV and cancers associated with HPV. The bill as amended by the

Health Subcommittee would also reauthorize and enhance Johanna's Law,[1] an existing CDC program aimed at preventing and increasing awareness of gynecologic cancers.

On July 15, 2021, the Subcommittee on Health favorably forwarded H.R. 1550, as amended, to the full Committee by a voice vote.

XI. H.R. 951, THE "MATERNAL VACCINATION ACT"

H.R. 951, the "Maternal Vaccination Act", introduced by Rep. Sewell (D-AL) and 44 original cosponsors, would extend vaccine outreach efforts to pregnant and postpartum individuals and obstetric care providers.[2] The existing vaccine outreach authorization would be increased by $2 million, to $17 million.

On July 15, 2021, the Subcommittee on Health favorably forwarded H.R. 951, as amended, to the full Committee by a voice vote.

XII. H.R. 4387, THE "MATERNAL HEALTH QUALITY IMPROVEMENT ACT OF 2021"

H.R. 4387, the "Maternal Health Quality Improvement Act of 2021", introduced by Reps. Kelly (D-IL), Bucshon, Adams (D-NC), Burgess, Hayes (D-CT), and Latta (R-OH), amends the Public Health Service Act to authorize grant funding to identify, develop, or disseminate best practices to improve maternal health quality and outcomes and eliminate preventable maternal mortality and severe maternal morbidity. The bill also establishes a grant program to award funding to accredited health professional schools for the training of health care professionals in order improve the provision of maternal health care with respect to perceptions and biases that may affect care.

Additionally, H.R. 4387 authorizes a competitive grant program to support perinatal quality collaboratives to improve perinatal care and health outcomes for pregnant and postpartum women and their infants. The bill also permits the Secretary of HHS to award grants to States, Indian Tribes, and Tribal organizations to deliver integrated health care services to pregnant and postpartum women. Finally, the legislation also includes provisions to improve rural maternal and obstetric care, including data collection and care networks, as well as telehealth resources and training.

On July 15, 2021, the Subcommittee on Health favorably forwarded H.R. 4387, without amendment, to the full Committee by a voice vote.

XIII. H.R. 3742, THE "VACCINE INFORMATION FOR NURSING FACILITY OPERATORS ACT" (THE "VACCINE INFO ACT")

---

[1] 42 U.S.C. 247b-17(d).

[2] Pub. L. No. 116-260.

H.R. 3742, the "Vaccine INFO Act", introduced by Reps. Bilirakis and Rice (D-NY), would require the Secretary of HHS to issue revised regulations requiring dissemination of information to staff on routine vaccines recommended by the Advisory Committee on Immunization Practices (ACIP) for health care personnel, including information on the benefits and potential side effects of receiving the vaccines and where they may receive the vaccines. This bill incorporates agency technical assistance.

On July 15, 2021, the Subcommittee on Health favorably forwarded H.R. 3742, as amended, to the full Committee by a voice vote.

XIV. H.R. 2347, THE "STRENGTHENING THE VACCINES FOR CHILDREN ACT OF 2021"

H.R. 2347, the "Strengthening the Vaccines for Children Act of 2021", introduced by Reps. Schrier, Butterfield (D-NC), McKinley (R-WV), and Joyce, would enhance the Vaccines for Children Program, which provides ACIP-recommended vaccines to low-income children. These enhancements include extending eligibility to children enrolled in CHIP, making changes to ensure adequate payment for multi-component vaccines, and providing an eight-quarter federal medical assistance percentage (FMAP) increase for expenditures on vaccines for beneficiaries under age 19, among other programmatic changes. The bill would also require the CDC to publicly report information related to demographic data of those vaccinated under the program and require a GAO study on the analysis of the effects of the bill's provisions on vaccination rates and provider participation.

On July 15, 2021, the Subcommittee on Health favorably forwarded H.R. 2347, as amended, to the full Committee by a voice vote.

XV. H.R. 3894, THE "COLLECTING AND ANALYZING RESOURCES INTEGRAL AND NECESSARY FOR GUIDANCE FOR SOCIAL DETERMINANTS ACT OF 2021" (THE "CARING FOR SOCIAL DETERMINANTS ACT OF 2021")

H.R. 3894, the "CARING for Social Determinants Act of 2021", introduced by Reps. Blunt Rochester and Bilirakis, requires the Secretary of HHS to provide guidance and technical assistance to states on how to address social determinants of health through Medicaid and the Children's Health Insurance Program (CHIP). It requires that the guidance be updated every three years. This bill also incorporates agency technical assistance.

On July 15, 2021, the Subcommittee on Health favorably forwarded H.R. 3894, as amended, to the full Committee by a voice vote.

XVI. H.R. 4406, THE "SUPPORTING MEDICAID IN THE U.S. TERRITORIES ACT"

H.R. 4406, the "Supporting Medicaid in the U.S. Territories Act", introduced by Reps. Soto (D-FL) and Bilirakis, and five original co-sponsors, would provide five years of enhanced Medicaid funding for Puerto Rico, and eight years of enhanced Medicaid funding for the U.S. Virgin Islands, American Samoa, the Commonwealth of the Northern Mariana Islands, and

Guam. It would extend the current enhanced FMAP for each of the territories for the length of the time of the increased funding. It would also make certain programmatic improvements to the Puerto Rico Medicaid program, including requiring increased provider payment rates, strengthening program integrity, and improving contracting practices.

On July 15, 2021, the Subcommittee on Health favorably forwarded H.R. 4406, without amendment, to the full Committee by a voice vote.

XVII. H.R. 2685, THE "UNDERSTANDING CYBERSECURITY OF MOBILE NETWORKS ACT"

H.R. 2685, the "Understanding Cybersecurity of Mobile Networks Act", introduced by Reps. Eshoo and Kinzinger (R-IL), would require the National Telecommunications and Information Administration (NTIA) to examine and report on the cybersecurity of mobile service networks and the vulnerability of these networks and mobile devices to cyberattacks and surveillance conducted by adversaries. The report must include an assessment of the degree to which providers of mobile service have addressed certain cybersecurity vulnerabilities; a discussion of the degree to which these providers have implemented cybersecurity best practices and risk assessment frameworks; and an estimate of the prevalence and efficacy of encryption and authentication algorithms and techniques used in mobile service and communications equipment, mobile devices, and mobile operating systems and software, among other things.

An Amendment in the Nature of a Substitute (AINS) is expected to be offered to make technical changes to the bill.

XVIII. H.R. 3919, THE "SECURE EQUIPMENT ACT OF 2021"

H.R. 3919, the "Secure Equipment Act of 2021", introduced by Reps. Scalise (R-LA) and Eshoo, would direct the Federal Communications Commission (FCC) to clarify that it will no longer review or approve applications from companies on the Commission's "Covered List." The bill would prevent further integration and sales of Huawei, ZTE, Hytera, Hikvision, and Dahua – all Chinese state-backed or directed firms – in the United States regardless of whether federal funds are involved.

An AINS is expected to be offered to clarify that the rules required by the legislation should not apply retroactively to equipment previously authorized by the FCC, and that the legislation does not prevent the FCC from studying whether, in a future proceeding, the rules should apply retroactively.

XIX. H.R. 4028, THE "INFORMATION AND COMMUNICATION TECHNOLOGY STRATEGY ACT"

H.R. 4028, the Information and Communication Technology Strategy Act", introduced by Reps. Long (R-MO), Spanberger (D-VA), Carter (R-GA), and McNerney (D-CA), would direct the Secretary of Commerce to submit to Congress within one year a report analyzing the state of economic competitiveness of trusted vendors in the information and communication technology supply chain, identifying which components or technologies are critical or

vulnerable, and identifying which components or technologies on which U.S. networks depend. It would also require the Secretary to submit to Congress, within six months after the report is submitted, a whole-of-government strategy to ensure the competitiveness of trusted vendors in the United States.

An AINS is expected to be offered to make technical changes to the bill.

XX. H.R. 4032, THE "OPEN RAN OUTREACH ACT"

H.R. 4032, the "Open RAN Outreach Act", introduced by Reps. Allred (D-TX), O'Halleran (D-AZ), Guthrie, and Hudson, directs the NTIA Administrator to provide outreach and technical assistance to small communications network providers regarding Open Radio Access Networks (Open-RAN).

An AINS is expected to be offered to clarify that the outreach and technical assistance should address the uses, benefits, and shortcoming of Open RAN; that the technical assistance may be related to participation in the grant program authorized in the FY 2021 National Defense Authorization Act; and that NTIA may use such grant funds to carry out the legislation.

XXI. H.R. 4045, THE "FUTURE USES OF TECHNOLOGY UPHOLDING RELIABLE AND ENHANCED NETWORKS ACT" (THE "FUTURE NETWORKS" ACT)

H.R. 4045, the "FUTURE Networks Act", introduced by Reps. Doyle (D-PA), Johnson (R-OH), and McBath (D-GA), would require the FCC to create a 6G (sixth-generation) Task Force. The bill stipulates that the membership of the Task Force shall be appointed by the FCC Chair, and that the Task Force membership be composed, if possible, of representatives from trusted companies (meaning those not controlled by foreign adversaries), trusted public interest groups, and trusted government representatives with at least one representative from federal, state, local, and tribal governments. The Task Force would have to submit a report to Congress on 6G wireless technology, including the possible uses, strengths, and limitations of 6G, (including any supply chain, cybersecurity, or other limitations that will need to be addressed in future generations of wireless technologies.

An AINS is expected to be offered to make technical changes to the bill.

XXII. H.R. 4046, THE "NTIA POLICY AND CYBERSECURITY COORDINATION ACT"

H.R. 4046, the "NTIA Policy and Cybersecurity Coordination Act", introduced by Reps. Duncan (R-SC), Wild (D-PA) and Curtis, would authorize the existing NTIA Office of Policy Analysis and Development and rename it the Office of Policy Development and Cybersecurity. In addition to codifying the responsibilities of NTIA in administering the information sharing program in Section 8 of the Secure and Trusted Communications Act, the Office would be assigned functions to coordinate and develop policy regarding the cybersecurity of communications networks.

An AINS is expected to be offered to make technical changes to the bill.

XXIII. H.R. 4055, THE "AMERICAN CYBERSECURITY LITERACY ACT"

H.R. 4055, the "American Cybersecurity Literacy Act", introduced by Reps. Kinzinger, Eshoo, Veasey (D-TX), Houlahan (D-PA), and Bilirakis, would require NTIA to develop and conduct a cybersecurity literacy campaign to educate U.S. individuals and businesses about common cybersecurity risks and best practices.

An AINS is expected to be offered to make technical changes to the bill.

XXIV. H.R. 4067, THE "COMMUNICATIONS SECURITY ADVISORY ACT OF 2021"

H.R. 4067, the "Communications Security Advisory Act of 2021", introduced by Reps. Slotkin (D-MI), Schrader (D-OR) and Walberg (R-MI), would codify an existing FCC advisory council, the Communications Security, Reliability, and Interoperability Council, focused on network security, resiliency, and interoperability. It also requires biennial reporting to the FCC, Congress, and public with recommendations to improve communications networks on such issues.

An AINS is expected to be offered to make technical changes to the bill.

STATUTORY ADDENDUM

CONTENTS

28 U.S.C. § 2344.....1
47 U.S.C. § 151.....1
47 U.S.C. § 154.....2
47 U.S.C. § 229.....14
47 U.S.C. § 302a.....15
47 U.S.C. § 303.....19
47 U.S.C. § 1004.....19
47 U.S.C. § 1302.....20

Pub. L. No. 115-232 21
Pub. L. No. 116-124 25
Pub. L. No. 117-55 31

47 C.F.R. § 1.401.....33

28 U.S.C. § 2344

§ 2344. Review of orders; time; notice; contents of petition; service

On the entry of a final order reviewable under this chapter, the agency shall promptly give notice thereof by service or publication in accordance with its rules. Any party aggrieved by the final order may, within 60 days after its entry, file a petition to review the order in the court of appeals wherein venue lies. The action shall be against the United States. The petition shall contain a concise statement of--

(1) the nature of the proceedings as to which review is sought;

(2) the facts on which venue is based;

(3) the grounds on which relief is sought; and

(4) the relief prayed.

The petitioner shall attach to the petition, as exhibits, copies of the order, report, or decision of the agency. The clerk shall serve a true copy of the petition on the agency and on the Attorney General by registered mail, with request for a return receipt.

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. § 154

§ 154. Federal Communications Commission

(a) Number of commissioners; appointment

The Federal Communications Commission (in this chapter referred to as the "Commission") shall be composed of five commissioners appointed by the President, by and with the advice and consent of the Senate, one of whom the President shall designate as chairman.

(b) Qualifications

(1) Each member of the Commission shall be a citizen of the United States.

(2)(A) No member of the Commission or person employed by the Commission shall--

(i) be financially interested in any company or other entity engaged in the manufacture or sale of telecommunications equipment which is subject to regulation by the Commission;

(ii) be financially interested in any company or other entity engaged in the business of communication by wire or radio or in the use of the electromagnetic spectrum;

(iii) be financially interested in any company or other entity which controls any company or other entity specified in clause (i) or clause (ii), or which derives a significant portion of its total income from ownership of stocks, bonds, or other securities of any such company or other entity; or

(iv) be employed by, hold any official relation to, or own any stocks, bonds, or other securities of, any person significantly regulated by the Commission under this chapter;

except that the prohibitions established in this subparagraph shall apply only to financial interests in any company or other entity which has a significant interest in communications, manufacturing, or sales activities which are subject to regulation by the Commission.

(B)(i) The Commission shall have authority to waive, from time to time, the application of the prohibitions established in subparagraph (A) to persons employed by the Commission if the Commission determines that the financial interests of a person which are involved in a particular case are minimal, except that such waiver authority shall be subject to the provisions of section 208 of Title 18. The waiver authority established in this subparagraph shall not apply with respect to members of the Commission.

(ii) In any case in which the Commission exercises the waiver authority established in this subparagraph, the Commission shall publish notice of such action in the Federal Register.

(3) The Commission, in determining whether a company or other entity has a significant interest in communications, manufacturing, or sales activities which are subject to regulation by the Commission, shall consider (without excluding other relevant factors)--

(A) the revenues, investments, profits, and managerial efforts directed to the related communications, manufacturing, or sales activities of the company or other entity involved, as compared to the other aspects of the business of such company or other entity;

(B) the extent to which the Commission regulates and oversees the activities of such company or other entity;

(C) the degree to which the economic interests of such company or other entity may be affected by any action of the Commission; and

(D) the perceptions held by the public regarding the business activities of such company or other entity.

(4) Members of the Commission shall not engage in any other business, vocation, profession, or employment while serving as such members.

(5) The maximum number of commissioners who may be members of the same political party shall be a number equal to the least number of commissioners which constitutes a majority of the full membership of the Commission.

(c) Terms of office; vacancies

(1) A commissioner--

(A) shall be appointed for a term of 5 years;

(B) except as provided in subparagraph (C), may continue to serve after the expiration of the fixed term of office of the commissioner until a successor is appointed and has been confirmed and taken the oath of office; and

(C) may not continue to serve after the expiration of the session of Congress that begins after the expiration of the fixed term of office of the commissioner.

(2) Any person chosen to fill a vacancy in the Commission--

(A) shall be appointed for the unexpired term of the commissioner that the person succeeds;

(B) except as provided in subparagraph (C), may continue to serve after the expiration of the fixed term of office of the commissioner that the person succeeds until a successor is appointed and has been confirmed and taken the oath of office; and

(C) may not continue to serve after the expiration of the session of Congress that begins after the expiration of the fixed term of office of the commissioner that the person succeeds.

(3) No vacancy in the Commission shall impair the right of the remaining commissioners to exercise all the powers of the Commission.

(d) Compensation of Commission members

Each Commissioner shall receive an annual salary at the annual rate payable from time to time for level IV of the Executive Schedule, payable in monthly installments. The Chairman of the Commission, during the period of his service as Chairman, shall receive an annual salary at the annual rate payable from time to time for level III of the Executive Schedule.

(e) Principal office; special sessions

The principal office of the Commission shall be in the District of Columbia, where its general sessions shall be held; but whenever the convenience of the public or of the parties may be promoted or delay or expense prevented thereby, the Commission may hold special sessions in any part of the United States.

(f) Employees and assistants; compensation of members of Field Engineering and Monitoring Bureau; use of amateur volunteers for certain purposes; commercial radio operator examinations

(1) The Commission shall have authority, subject to the provisions of the civil-service laws and chapter 51 and subchapter III of chapter 53 of Title 5, to appoint such officers, engineers, accountants, attorneys, inspectors, examiners, and other employees as are necessary in the exercise of its functions.

(2) Without regard to the civil-service laws, but subject to chapter 51 and subchapter III of chapter 53 of Title 5, each commissioner may appoint three professional assistants and a secretary, each of whom shall perform such duties as such commissioner shall

direct. In addition, the chairman of the Commission may appoint, without regard to the civil-service laws, but subject to chapter 51 and subchapter III of chapter 53 of Title 5, an administrative assistant who shall perform such duties as the chairman shall direct.

(3) The Commission shall fix a reasonable rate of extra compensation for overtime services of engineers in charge and radio engineers of the Field Engineering and Monitoring Bureau of the Federal Communications Commission, who may be required to remain on duty between the hours of 5 o'clock postmeridian and 8 o'clock antemeridian or on Sundays or holidays to perform services in connection with the inspection of ship radio equipment and apparatus for the purposes of part II of subchapter III of this chapter or the Great Lakes Agreement, on the basis of one-half day's additional pay for each two hours or fraction thereof of at least one hour that the overtime extends beyond 5 o'clock postmeridian (but not to exceed two and one-half days' pay for the full period from 5 o'clock postmeridian to 8 o'clock antemeridian) and two additional days' pay for Sunday or holiday duty. The said extra compensation for overtime services shall be paid by the master, owner, or agent of such vessel to the local United States collector of customs or his representative, who shall deposit such collection into the Treasury of the United States to an appropriately designated receipt account: *Provided*, That the amounts of such collections received by the said collector of customs or his representatives shall be covered into the Treasury as miscellaneous receipts; and the payments of such extra compensation to the several employees entitled thereto shall be made from the annual appropriations for salaries and expenses of the Commission: *Provided further*, That to the extent that the annual appropriations which are authorized to be made from the general fund of the Treasury are insufficient, there are authorized to be appropriated from the general fund of the Treasury such additional amounts as may be necessary to the extent that the amounts of such receipts are in excess of the amounts

appropriated: *Provided further*, That such extra compensation shall be paid if such field employees have been ordered to report for duty and have so reported whether the actual inspection of the radio equipment or apparatus takes place or not: *And provided further*, That in those ports where customary working hours are other than those hereinabove mentioned, the engineers in charge are vested with authority to regulate the hours of such employees so as to agree with prevailing working hours in said ports where inspections are to be made, but nothing contained in this proviso shall be construed in any manner to alter the length of a working day for the engineers in charge and radio engineers or the overtime pay herein fixed: and *Provided further*, That, in the alternative, an entity designated by the Commission may make the inspections referred to in this paragraph.

(4)(A) The Commission, for purposes of preparing or administering any examination for an amateur station operator license, may accept and employ the voluntary and uncompensated services of any individual who holds an amateur station operator license of a higher class than the class of license for which the examination is being prepared or administered. In the case of examinations for the highest class of amateur station operator license, the Commission may accept and employ such services of any individual who holds such class of license.

(B)(i) The Commission, for purposes of monitoring violations of any provision of this chapter (and of any regulation prescribed by the Commission under this chapter) relating to the amateur radio service, may--

(I) recruit and train any individual licensed by the Commission to operate an amateur station; and

(II) accept and employ the voluntary and uncompensated services of such individual.

(ii) The Commission, for purposes of recruiting and training individuals under clause (i) and for purposes of screening, annotating, and summarizing violation reports referred under clause (i), may accept and employ the voluntary and uncompensated services of any amateur station operator organization.

(iii) The functions of individuals recruited and trained under this subparagraph shall be limited to--

(I) the detection of improper amateur radio transmissions;

(II) the conveyance to Commission personnel of information which is essential to the enforcement of this chapter (or regulations prescribed by the Commission under this chapter) relating to the amateur radio service; and

(III) issuing advisory notices, under the general direction of the Commission, to persons who apparently have violated any provision of this chapter (or regulations prescribed by the Commission under this chapter) relating to the amateur radio service.

Nothing in this clause shall be construed to grant individuals recruited and trained under this subparagraph any authority to issue sanctions to violators or to take any enforcement action other than any action which the Commission may prescribe by rule.

(C)(i) The Commission, for purposes of monitoring violations of any provision of this chapter (and of any regulation prescribed by the Commission under this chapter) relating to the citizens band radio service, may--

(I) recruit and train any citizens band radio operator; and

(II) accept and employ the voluntary and uncompensated services of such operator.

(ii) The Commission, for purposes of recruiting and training individuals under clause (i) and for purposes of screening, annotating, and summarizing violation reports referred under clause (i), may accept and employ the voluntary and uncompensated services of any citizens band radio operator organization. The Commission, in accepting and employing services of individuals under this subparagraph, shall seek to achieve a broad representation of individuals and organizations interested in citizens band radio operation.

(iii) The functions of individuals recruited and trained under this subparagraph shall be limited to--

(I) the detection of improper citizens band radio transmissions;

(II) the conveyance to Commission personnel of information which is essential to the enforcement of this chapter (or regulations prescribed by the Commission under this chapter) relating to the citizens band radio service; and

(III) issuing advisory notices, under the general direction of the Commission, to persons who apparently have violated any provision of this chapter (or regulations prescribed by the Commission under this chapter) relating to the citizens band radio service.

Nothing in this clause shall be construed to grant individuals recruited and trained under this subparagraph any authority to issue sanctions to violators or to take any enforcement action other than any action which the Commission may prescribe by rule.

(D) The Commission shall have the authority to endorse certification of individuals to perform transmitter installation, operation, maintenance, and repair duties in the private land mobile services and fixed services (as defined by the Commission by rule) if such certification programs are conducted by organizations or committees which are representative of the users in those services and which consist of individuals who are not officers or employees of the Federal Government.

(E) The authority of the Commission established in this paragraph shall not be subject to or affected by the provisions of part III of Title 5 or section 1342 of Title 31.

(F) Any person who provides services under this paragraph shall not be considered, by reason of having provided such services, a Federal employee.

(G) The Commission, in accepting and employing services of individuals under subparagraphs (A) and (B), shall seek to achieve a broad representation of individuals and organizations interested in amateur station operation.

(H) The Commission may establish rules of conduct and other regulations governing the service of individuals under this paragraph.

(I) With respect to the acceptance of voluntary uncompensated services for the preparation, processing, or administration of examinations for amateur station operator licenses pursuant to subparagraph (A) of this paragraph, individuals, or organizations which provide or coordinate such authorized volunteer services may recover from examinees reimbursement for out-of-pocket costs.

(5)(A) The Commission, for purposes of preparing and administering any examination for a commercial radio operator license or endorsement, may accept and employ the services of persons that the Commission determines to be qualified. Any

person so employed may not receive compensation for such services, but may recover from examinees such fees as the Commission permits, considering such factors as public service and cost estimates submitted by such person.

(B) The Commission may prescribe regulations to select, oversee, sanction, and dismiss any person authorized under this paragraph to be employed by the Commission.

(C) Any person who provides services under this paragraph or who provides goods in connection with such services shall not, by reason of having provided such service or goods, be considered a Federal or special government employee.

(g) Expenditures

(1) The Commission may make such expenditures (including expenditures for rent and personal services at the seat of government and elsewhere, for office supplies, law books, periodicals, and books of reference, for printing and binding, for land for use as sites for radio monitoring stations and related facilities, including living quarters where necessary in remote areas, for the construction of such stations and facilities, and for the improvement, furnishing, equipping, and repairing of such stations and facilities and of laboratories and other related facilities (including construction of minor subsidiary buildings and structures not exceeding $25,000 in any one instance) used in connection with technical research activities), as may be necessary for the execution of the functions vested in the Commission and as may be appropriated for by the Congress in accordance with the authorizations of appropriations established in section 156 of this title. All expenditures of the Commission, including all necessary expenses for transportation incurred by the commissioners or by their employees, under their orders, in making any investigation or upon any official business in any other places than in the city of Washington, shall be allowed and paid on the presentation of itemized vouchers therefor approved by the chairman of the

Commission or by such other member or officer thereof as may be designated by the Commission for that purpose.

(2) Repealed. Pub.L. 115-141, Div. P, Title IV, § 402(i)(1)(B), Mar. 23, 2018, 132 Stat. 1089

(3)(A) Notwithstanding any other provision of law, in furtherance of its functions the Commission is authorized to accept, hold, administer, and use unconditional gifts, donations, and bequests of real, personal, and other property (including voluntary and uncompensated services, as authorized by section 3109 of Title 5).

(B) The Commission, for purposes of providing radio club and military-recreational call signs, may utilize the voluntary, uncompensated, and unreimbursed services of amateur radio organizations authorized by the Commission that have tax-exempt status under section 501(c)(3) of Title 26.

(C) For the purpose of Federal law on income taxes, estate taxes, and gift taxes, property or services accepted under the authority of subparagraph (A) shall be deemed to be a gift, bequest, or devise to the United States.

(D) The Commission shall promulgate regulations to carry out the provisions of this paragraph. Such regulations shall include provisions to preclude the acceptance of any gift, bequest, or donation that would create a conflict of interest or the appearance of a conflict of interest.

(h) Quorum; seal

Three members of the Commission shall constitute a quorum thereof. The Commission shall have an official seal which shall be judicially noticed.

(i) Duties and powers

The Commission may perform any and all acts, make such rules and regulations, and issue such orders, not inconsistent with this chapter, as may be necessary in the execution of its functions.

(j) Conduct of proceedings; hearings

The Commission may conduct its proceedings in such manner as will best conduce to the proper dispatch of business and to the ends of justice. No commissioner shall participate in any hearing or proceeding in which he has a pecuniary interest. Any party may appear before the Commission and be heard in person or by attorney. Every vote and official act of the Commission shall be entered of record, and its proceedings shall be public upon the request of any party interested. The Commission is authorized to withhold publication of records or proceedings containing secret information affecting the national defense.

(k) Record of reports

All reports of investigations made by the Commission shall be entered of record, and a copy thereof shall be furnished to the party who may have complained, and to any common carrier or licensee that may have been complained of.

(l) Publication of reports; admissibility as evidence

The Commission shall provide for the publication of its reports and decisions in such form and manner as may be best adapted for public information and use, and such authorized publications shall be competent evidence of the reports and decisions of the Commission therein contained in all courts of the United States and of the several States without any further proof or authentication thereof.

(m) Compensation of appointees

Rates of compensation of persons appointed under this section shall be subject to the reduction applicable to officers and employees of the Federal Government generally.

(n) Use of communications in safety of life and property

For the purpose of obtaining maximum effectiveness from the use of radio and wire communications in connection with safety of life and property, the Commission shall investigate and study all phases of the problem and the best methods of obtaining the cooperation and coordination of these systems.

(o) Redesignated (n)

47 U.S.C. § 229

§ 229. Communications Assistance for Law Enforcement Act compliance

(a) In general

The Commission shall prescribe such rules as are necessary to implement the requirements of the Communications Assistance for Law Enforcement Act.

(b) Systems security and integrity

The rules prescribed pursuant to subsection (a) shall include rules to implement section 105 of the Communications Assistance for Law Enforcement Act that require common carriers--

> **(1)** to establish appropriate policies and procedures for the supervision and control of its officers and employees--
>
> > **(A)** to require appropriate authorization to activate interception of communications or access to call-identifying information; and
> >
> > **(B)** to prevent any such interception or access without such authorization;
>
> **(2)** to maintain secure and accurate records of any interception or access with or without such authorization; and

(3) to submit to the Commission the policies and procedures adopted to comply with the requirements established under paragraphs (1) and (2).

* * *

47 U.S.C. § 302a

§ 302a. Devices which interfere with radio reception

(a) Regulations

The Commission may, consistent with the public interest, convenience, and necessity, make reasonable regulations (1) governing the interference potential of devices which in their operation are capable of emitting radio frequency energy by radiation, conduction, or other means in sufficient degree to cause harmful interference to radio communications; and (2) establishing minimum performance standards for home electronic equipment and systems to reduce their susceptibility to interference from radio frequency energy. Such regulations shall be applicable to the manufacture, import, sale, offer for sale, or shipment of such devices and home electronic equipment and systems, and to the use of such devices.

(b) Restrictions

No person shall manufacture, import, sell, offer for sale, or ship devices or home electronic equipment and systems, or use devices, which fail to comply with regulations promulgated pursuant to this section.

(c) Exceptions

The provisions of this section shall not be applicable to carriers transporting such devices or home electronic equipment and systems without trading in them, to devices or home electronic equipment and systems manufactured solely for export, to the manufacture, assembly, or installation of devices or home electronic equipment and systems for its own use by a public utility engaged in providing electric service, or to devices or home electronic equipment and systems for use by the

Government of the United States or any agency thereof. Devices and home electronic equipment and systems for use by the Government of the United States or any agency thereof shall be developed, procured, or otherwise acquired, including offshore procurement, under United States Government criteria, standards, or specifications designed to achieve the objectives of reducing interference to radio reception and to home electronic equipment and systems, taking into account the unique needs of national defense and security.

(d) Cellular telecommunications receivers

(1) Within 180 days after October 28, 1992, the Commission shall prescribe and make effective regulations denying equipment authorization (under part 15 of title 47, Code of Federal Regulations, or any other part of that title) for any scanning receiver that is capable of--

(A) receiving transmissions in the frequencies allocated to the domestic cellular radio telecommunications service,

(B) readily being altered by the user to receive transmissions in such frequencies, or

(C) being equipped with decoders that convert digital cellular transmissions to analog voice audio.

(2) Beginning 1 year after the effective date of the regulations adopted pursuant to paragraph (1), no receiver having the capabilities described in subparagraph (A), (B), or (C) of paragraph (1), as such capabilities are defined in such regulations, shall be manufactured in the United States or imported for use in the United States.

(e) Delegation of equipment testing and certification to private laboratories

The Commission may--

(1) authorize the use of private organizations for testing and certifying the compliance of devices or home electronic equipment and systems with regulations promulgated under this section;

(2) accept as prima facie evidence of such compliance the certification by any such organization; and

(3) establish such qualifications and standards as it deems appropriate for such private organizations, testing, and certification.

(f) State and local enforcement of FCC regulations on use of citizens band radio equipment

(1) Except as provided in paragraph (2), a State or local government may enact a statute or ordinance that prohibits a violation of the following regulations of the Commission under this section:

(A) A regulation that prohibits a use of citizens band radio equipment not authorized by the Commission.

(B) A regulation that prohibits the unauthorized operation of citizens band radio equipment on a frequency between 24 MHz and 35 MHz.

(2) A station that is licensed by the Commission pursuant to section 301 of this title in any radio service for the operation at issue shall not be subject to action by a State or local government under this subsection. A State or local government statute or ordinance enacted for purposes of this subsection shall identify the exemption available under this paragraph.

(3) The Commission shall, to the extent practicable, provide technical guidance to State and local governments regarding the detection and determination of violations of the regulations specified in paragraph (1).

(4)(A) In addition to any other remedy authorized by law, a person affected by the decision of a State or local government

agency enforcing a statute or ordinance under paragraph (1) may submit to the Commission an appeal of the decision on the grounds that the State or local government, as the case may be, enacted a statute or ordinance outside the authority provided in this subsection.

(B) A person shall submit an appeal on a decision of a State or local government agency to the Commission under this paragraph, if at all, not later than 30 days after the date on which the decision by the State or local government agency becomes final, but prior to seeking judicial review of such decision.

(C) The Commission shall make a determination on an appeal submitted under subparagraph (B) not later than 180 days after its submittal.

(D) If the Commission determines under subparagraph (C) that a State or local government agency has acted outside its authority in enforcing a statute or ordinance, the Commission shall preempt the decision enforcing the statute or ordinance.

(5) The enforcement of statute or ordinance that prohibits a violation of a regulation by a State or local government under paragraph (1) in a particular case shall not preclude the Commission from enforcing the regulation in that case concurrently.

(6) Nothing in this subsection shall be construed to diminish or otherwise affect the jurisdiction of the Commission under this section over devices capable of interfering with radio communications.

(7) The enforcement of a statute or ordinance by a State or local government under paragraph (1) with regard to citizens band radio equipment on board a "commercial motor vehicle", as defined in section 31101 of Title 49, shall require probable cause to find that the commercial motor vehicle or the individual operating the

vehicle is in violation of the regulations described in paragraph (1).

47 U.S.C. § 303

§ 303. Powers and duties of Commission

Except as otherwise provided in this chapter, the Commission from time to time, as public convenience, interest, or necessity requires, shall--

(a) Classify radio stations;

(b) Prescribe the nature of the service to be rendered by each class of licensed stations and each station within any class;

(c) Assign bands of frequencies to the various classes of stations, and assign frequencies for each individual station and determine the power which each station shall use and the time during which it may operate;

(d) Determine the location of classes of stations or individual stations;

(e) Regulate the kind of apparatus to be used with respect to its external effects and the purity and sharpness of the emissions from each station and from the apparatus therein;

* * *

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.

47 U.S.C. § 1302

§ 1302. Advanced telecommunications incentives

(a) In general

The Commission and each State commission with regulatory jurisdiction over telecommunications services shall encourage the deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans (including, in particular, elementary and secondary schools and classrooms) by utilizing, in a manner consistent with the public interest, convenience, and necessity, price cap regulation, regulatory forbearance, measures that promote competition in the local telecommunications market, or other regulating methods that remove barriers to infrastructure investment.

(b) Inquiry

The Commission shall, within 30 months after February 8, 1996, and annually thereafter, initiate a notice of inquiry concerning the availability of advanced telecommunications capability to all Americans (including, in particular, elementary and secondary schools and classrooms) and shall complete the inquiry within 180 days after its initiation. In the inquiry, the Commission shall determine whether advanced telecommunications capability is being deployed to all Americans in a reasonable and timely fashion. If the Commission's determination is negative, it shall take immediate action to accelerate deployment of such capability by removing barriers to infrastructure investment and by promoting competition in the telecommunications market.

(c) Demographic information for unserved areas

As part of the inquiry required by subsection (b), the Commission shall compile a list of geographical areas that are not served by any provider of advanced telecommunications capability (as defined by subsection (d)(1)) and to the extent that data from the Census Bureau is available, determine, for each such unserved area--

(1) the population;

(2) the population density; and

(3) the average per capita income.

(d) Definitions

For purposes of this subsection:[1]

(1) Advanced telecommunications capability

The term "advanced telecommunications capability" is defined, without regard to any transmission media or technology, as high-speed, switched, broadband telecommunications capability that enables users to originate and receive high-quality voice, data, graphics, and video telecommunications using any technology.

(2) Elementary and secondary schools

The term "elementary and secondary schools" means elementary and secondary schools, as defined in section 7801 of Title 20.

UNITED STATES PUBLIC LAWS
115th Congress - Second Session
Convening January 06, 2018

August 13, 2018

JOHN S. MCCAIN NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2019

* * *

SEC. 889. PROHIBITION ON CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT.

(a) PROHIBITION ON USE OR PROCUREMENT.—(1) The head of an executive agency may not—

(A) procure or obtain or extend or renew a contract to procure or obtain any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system; or

(B) enter into a contract (or extend or renew a contract) with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system.

(2) Nothing in paragraph (1) shall be construed to—

(A) prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(B) cover telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(b) PROHIBITION ON LOAN AND GRANT FUNDS.—(1) The head of an executive agency may not obligate or expend loan or grant funds to procure or obtain, extend or renew a contract to procure or obtain, or enter into a contract (or extend or renew a contract) to procure or obtain the equipment, services, or systems described in subsection (a).

(2) In implementing the prohibition in paragraph (1), heads of executive agencies administering loan, grant, or subsidy programs, including the heads of the Federal Communications Commission, the Department of Agriculture, the Department of Homeland Security, the Small Business Administration, and the Department of Commerce, shall prioritize available funding and technical support to assist affected businesses, institutions and organizations as is reasonably necessary for those affected entities to transition from covered communications equipment and

services, to procure replacement equipment and services, and to ensure that communications service to users and customers is sustained.

(3) Nothing in this subsection shall be construed to—

(A) prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(B) cover telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(c) EFFECTIVE DATES.—The prohibition under subsection (a)(1)(A) shall take effect one year after the date of the enactment of this Act, and the prohibitions under subsections (a)(1)(B) and (b)(1) shall take effect two years after the date of the enactment of this Act.

(d) WAIVER AUTHORITY.—

(1) EXECUTIVE AGENCIES.—The head of an executive agency may, on a one-time basis, waive the requirements under subsection (a) with respect to an entity that requests such a waiver. The waiver may be provided, for a period of not more than two years after the effective dates described in subsection (c), if the entity seeking the waiver—

(A) provides a compelling justification for the additional time to implement the requirements under such subsection, as determined by the head of the executive agency; and

(B) submits to the head of the executive agency, who shall not later than 30 days thereafter submit to the appropriate congressional committees, a full and complete laydown of the presences of covered telecommunications or video surveillance equipment or services in the entity's supply chain and a phase-out plan to eliminate such covered

telecommunications or video surveillance equipment or services from the entity's systems.

(2) DIRECTOR OF NATIONAL INTELLIGENCE.—The Director of National Intelligence may provide a waiver on a date later than the effective dates described in subsection (c) if the Director determines the waiver is in the national security interests of the United States.

(f) DEFINITIONS.—In this section:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term "appropriate congressional committees" means—

(A) the Committee on Banking, Housing, and Urban Affairs, the Committee on Foreign Relations, and the Committee on Homeland Security and Governmental Affairs of the Senate; and

(B) the Committee on Financial Services, the Committee on Foreign Affairs, and the Committee on Oversight and Government Reform of the House of Representatives.

(2) COVERED FOREIGN COUNTRY.—The term "covered foreign country" means the People's Republic of China.

(3) COVERED TELECOMMUNICATIONS EQUIPMENT OR SERVICES.—The term "covered telecommunications equipment or services" means any of the following:

(A) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities).

(B) For the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision

Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities).

(C) Telecommunications or video surveillance services provided by such entities or using such equipment.

(D) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of the National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

(4) EXECUTIVE AGENCY.—The term "executive agency" has the meaning given the term in section 133 of title 41, United States Code.

UNITED STATES PUBLIC LAWS
116th Congress - Second Session
Convening January 03, 2020
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,

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, *159 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, *160 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.

SEC. 10. SEVERABILITY.

If any provision of this Act, or the application of such a provision to any person or circumstance, is held to be unconstitutional, the remaining provisions of this Act, and the application of such provisions to any person or circumstance, shall not be affected thereby.

SEC. 11. DETERMINATION OF BUDGETARY EFFECTS.

The budgetary effects of this Act, for the purpose of complying with the Statutory Pay-As-You-Go Act of 2010, shall be determined by reference to the latest statement titled "Budgetary Effects of PAYGO Legislation"

for this Act, submitted for printing in the Congressional Record by the Chairman of the House Budget Committee, provided that such statement has been submitted prior to the vote on passage.

UNITED STATES PUBLIC LAWS
117th Congress - First Session
Convening January 21, 2021

November 11, 2021

SECURE EQUIPMENT ACT OF 2021

An Act To ensure that the Federal Communications Commission prohibits authorization of radio frequency devices that pose a national security risk.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Secure Equipment Act of 2021".

SEC. 2. UPDATES TO EQUIPMENT AUTHORIZATION PROCESS OF FEDERAL COMMUNICATIONS COMMISSION.

(a) RULEMAKING.—

(1) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, the Commission shall adopt rules in the proceeding initiated in the Notice of Proposed Rulemaking in the matter of Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program (ET Docket No. 21–232; FCC 21–73; adopted June 17, 2021), in accordance with paragraph (2), to

update the equipment authorization procedures of the Commission.

(2) UPDATES REQUIRED.—In the rules adopted under paragraph (1), the Commission shall clarify that the Commission will no longer review or approve any application for equipment authorization for equipment that is on the list of covered communications equipment or services published by the Commission under section 2(a) of the Secure and Trusted Communications Networks Act of 2019 (47 U.S.C. 1601(a)).

(3) APPLICABILITY.—

(A) IN GENERAL.—In the rules adopted under paragraph (1), the Commission may not provide for review or revocation of any equipment authorization granted before the date on which such rules are adopted on the basis of the equipment being on the list described in paragraph (2).

(B) RULE OF CONSTRUCTION.—Nothing in this section may be construed to prohibit the Commission, other than in the rules adopted under paragraph (1), from—

(i) examining the necessity of review or revocation of any equipment authorization on the basis of the equipment being on the list described in paragraph (2); or

(ii) adopting rules providing for any such review or revocation.

(b) DEFINITION.—In this section, the term "Commission" means the Federal Communications Commission.

47 C.F.R. § 1.401

§ 1.401 Petitions for rulemaking.

(a) Any interested person may petition for the issuance, amendment or repeal of a rule or regulation.

(b) The petition for rule making shall conform to the requirements of §§ 1.49, 1.52, and 1.419(b) (or § 1.420(e), if applicable), and shall be submitted or addressed to the Secretary, Federal Communications Commission, Washington, DC 20554, or may be submitted electronically.

(c) The petition shall set forth the text or substance of the proposed rule, amendment, or rule to be repealed, together with all facts, views, arguments and data deemed to support the action requested, and shall indicate how the interests of petitioner will be affected.

(d) Petitions for amendment of the FM Table of Assignments (§ 73.202 of this chapter) or the Television Table of Assignments (§ 73.606) shall be served by petitioner on any Commission licensee or permittee whose channel assignment would be changed by grant of the petition. The petition shall be accompanied by a certificate of service on such licensees or permittees. Petitions to amend the FM Table of Allotments must be accompanied by the appropriate construction permit application and payment of the appropriate application filing fee.

(e) Petitions which are moot, premature, repetitive, frivolous, or which plainly do not warrant consideration by the Commission may be denied or dismissed without prejudice to the petitioner.