

ORAL ARGUMENT NOT YET SCHEDULED

No. 25-1274

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

HIKVISION USA, INC.,
Petitioner,

v.

FEDERAL COMMUNICATIONS COMMISSION
and UNITED STATES OF AMERICA,
Respondents.

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

BRIEF FOR RESPONDENTS

Brett A. Shumate
Assistant Attorney General

Eric D. McArthur
*Deputy Assistant
Attorney General*

Sharon Swingle
Simon G. Jerome
Attorneys

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

D. Adam Candeub
General Counsel

Jacob M. Lewis
Deputy General Counsel

Sarah E. Citrin
Deputy Associate General Counsel

Scott M. Noveck
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.** The Petitioner is Hikvision USA, Inc. The Respondents are the Federal Communications Commission and the United States of America. The Intervenor in support of Respondents is Motorola Solutions, Inc.

(B) **Rulings Under Review.** The petition for review challenges the Federal Communications Commission's Second Report & Order and Second Further Notice of Proposed Rulemaking, *Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program*, FCC 25-71, 40 FCC Rcd. --- (rel. Oct. 29, 2025) (*2025 Order*), reprinted at JA____–____.

(C) **Related Cases.** The *2025 Order* under review has not previously been before this Court or any other court. A related challenge to an earlier order in the same agency docket, involving the same parties as this case, was previously decided by this Court in *Hikvision USA, Inc. v. FCC*, 97 F.4th 938 (D.C. Cir. 2024) (*Hikvision I*). 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	xii
INTRODUCTION	1
JURISDICTIONAL STATEMENT	3
STATEMENT OF THE ISSUES	4
PERTINENT STATUTES AND REGULATIONS	4
STATEMENT OF THE CASE	4
A. Foundational Mandates Of The Commission	4
B. The Secure Networks Act And The Covered List	8
C. The <i>2021 NPRM</i> And The Secure Equipment Act	10
D. The <i>2022 Order</i> And <i>Hikvision I</i>	14
E. The <i>2025 Order</i> Under Review	18
F. Subsequent Developments	22
STANDARD OF REVIEW	22
SUMMARY OF THE ARGUMENT	24
ARGUMENT	26
I. HIKVISION HAS NOT ESTABLISHED STANDING TO PURSUE ITS FACIAL CHALLENGE.	26
II. THE COMMISSION HAS AUTHORITY TO CONSIDER AND ADDRESS NATIONAL SECURITY RISKS THROUGH ITS EQUIPMENT AUTHORIZATION RULES, INCLUDING BY REVOKING OR LIMITING EXISTING AUTHORIZATIONS.	31
A. The Secure Equipment Act Confirms That The Commission May Base Equipment Authorization Decisions On National Security Concerns	31
B. The Secure Equipment Act Ratifies And Reinforces The Commission’s Preexisting Title III Authority.	41

TABLE OF CONTENTS
(continued)

	Page
CONCLUSION	52
CERTIFICATE OF COMPLIANCE.....	53

TABLE OF AUTHORITIES*

Cases	Page(s)
<i>All. for the Wild Rockies v. Salazar</i> , 672 F.3d 1170 (9th Cir. 2012)	32
<i>Am. Libr. Ass’n v. FCC</i> , 406 F.3d 689 (D.C. Cir. 2005)	44–45
<i>Am. Petrol. Inst. v. U.S. EPA</i> , 216 F.3d 50 (D.C. Cir. 2000)	28
<i>Ass’n of Flight Attendants v. U.S. DOT</i> , 564 F.3d 462 (D.C. Cir. 2009)	30–31
<i>Canonsburg Gen. Hosp. v. Burwell</i> , 807 F.3d 295 (D.C. Cir. 2015)	41
<i>Cellco P’ship v. FCC</i> , 700 F.3d 534 (D.C. Cir. 2012)	4
<i>Chamber of Com. of the U.S. v. EPA</i> , 642 F.3d 192 (D.C. Cir. 2011)	28
<i>China Telecom (Ams.) Corp. v. FCC</i> , 57 F.4th 256 (D.C. Cir. 2022).....	6, 7, 8, 23, 42
<i>China Unicom (Ams.) Ops. Ltd. v. FCC</i> , 124 F.4th 1128 (9th Cir. 2024)	8, 36–37, 42, 44
<i>Clapper v. Amnesty Int’l USA</i> , 568 U.S. 398 (2013).....	29
<i>Colo. Radio Corp. v. FCC</i> , 118 F.2d 24 (D.C. Cir. 1941)	35
* <i>Entergy Ark., LLC v. FERC</i> , 134 F.4th 576 (D.C. Cir. 2025).....	22, 27, 30

* *Authorities upon which this brief chiefly relies are marked with asterisks.*

TABLE OF AUTHORITIES

(continued)

	Page(s)
<i>FCC v. Nat’l Citizens Comm. for Broad.</i> , 436 U.S. 775 (1978).....	42
<i>FCC v. Prometheus Radio Project</i> , 592 U.S. 414 (2021).....	23
<i>FCC v. WNCN Listeners Guild</i> , 450 U.S. 582 (1981).....	42
<i>FDA v. All. for Hippocratic Medicine</i> , 602 U.S. 367 (2024).....	28
<i>Fogel v. Chestnutt</i> , 668 F.2d 100 (2d Cir. 1981)	34
<i>Friends of Animals v. Jewell</i> , 824 F.3d 1033 (D.C. Cir. 2016)	32
<i>Functional Music, Inc. v. FCC</i> , 274 F.2d 543 (D.C. Cir. 1959)	29
<i>Goodyear Atomic Corp. v. Miller</i> , 486 U.S. 174 (1988).....	37
<i>Haig v. Agee</i> , 453 U.S. 280 (1981).....	23, 36, 48
* <i>Hikvision USA, Inc. v. FCC (Hikvision I)</i> , 97 F.4th 938 (D.C. Cir. 2024).....	1, 3, 8, 9, 17–18, 25, 31, 33–34, 35, 41
* <i>Huawei Techs. USA, Inc. v. FCC</i> , 2 F.4th 421 (5th Cir. 2021)	6, 7, 8, 9, 42, 46, 48, 50, 51
<i>Kelly v. Robinson</i> , 479 U.S. 36 (1986).....	49

TABLE OF AUTHORITIES (continued)

	Page(s)
<i>Koons Buick Pontiac GMC, Inc. v. Nigh</i> , 543 U.S. 50 (2004).....	49
<i>Laffey v. Nw. Airlines</i> , 740 F.2d 1071 (D.C. Cir. 1984) (per curiam).....	34
<i>LaShawn A. v. Barry</i> , 87 F.3d 1389 (D.C. Cir. 1996) (en banc)	34
<i>Loper Bright Enters. v. Raimondo</i> , 603 U.S. 369 (2024).....	23
<i>Lujan v. Defs. of Wildlife</i> , 504 U.S. 555 (1992).....	27
<i>N.M. Att’y Gen. v. FERC</i> , 466 F.3d 120 (D.C. Cir. 2006) (per curiam).....	28
<i>Nat’l Broad. Co. v. United States</i> , 319 U.S. 190 (1943).....	43, 46
<i>Nat’l Cable & Telecomms. Ass’n v. FCC</i> , 567 F.3d 659 (D.C. Cir. 2009)	44
<i>Nw. Ind. Tel. Co. v. FCC</i> , 872 F.2d 465 (D.C. Cir. 1989)	34
<i>Omni Outdoor Advert., Inc. v. Columbia Outdoor Advert., Inc.</i> , 974 F.2d 502 (4th Cir. 1992).....	35
<i>Oncale v. Sundowner Offshore Oil Servs.</i> , 523 U.S. 75 (1998).....	44
<i>Pac. Networks Corp. v. FCC</i> , 77 F.4th 1160 (D.C. Cir. 2023).....	8, 42, 46
<i>Qwest Commc’ns Int’l, Inc. v. FCC</i> , 398 F.3d 1222 (10th Cir. 2005).....	47

TABLE OF AUTHORITIES
(continued)

	Page(s)
<i>Robertson v. Seattle Audubon Soc’y</i> , 503 U.S. 429 (1992).....	32–33
<i>Saline Parents v. Garland</i> , 88 F.4th 298 (D.C. Cir. 2023).....	28
<i>SEC v. Chenery Corp.</i> , 332 U.S. 194 (1947).....	41
* <i>Sierra Club v. EPA</i> , 292 F.3d 895 (D.C. Cir. 2002)	22, 27, 29
<i>SunCom Mobile & Data, Inc. v. FCC</i> , 87 F.3d 1386 (D.C. Cir. 1996)	29
<i>Trump v. New York</i> , 592 U.S. 125 (2020) (per curiam).....	28
<i>Twin Rivers Paper Co. v. SEC</i> , 934 F.3d 607 (D.C. Cir. 2019)	27
<i>United States v. Heinszen</i> , 206 U.S. 370 (1907).....	17
<i>United States v. Heirs of Boisdoré</i> , 49 U.S. (8 How.) 113 (1849)	49
<i>United States v. Speakman</i> , 594 F.3d 1165 (10th Cir. 2010).....	47
<i>Whitmore v. Arkansas</i> , 495 U.S. 149 (1990).....	29
<i>Williamsburg Wax Museum, Inc. v. Historical Figures, Inc.</i> , 810 F.2d 243 (D.C. Cir. 1987)	34

TABLE OF AUTHORITIES (continued)

Page(s)

Administrative Materials:

Executive Order No. 13913, 85 Fed. Reg. 19643 (Apr. 4, 2020)	7
<i>Process Reform for Exec. Branch Review of Certain FCC Appls. & Pets.</i> , 35 FCC Rcd. 10927 (2020).....	7
<i>Protecting Against Nat’l Sec. Threats to the Commc’ns Supply Chain</i> , 34 FCC Rcd. 11423 (2019)	9
<i>Rules & Pol’ys on Foreign Participation in the U.S. Telecomms. Mkt.</i> , 12 FCC Rcd. 23891 (1997).....	7

Statutes, Regulations, And Rules:

5 U.S.C. § 706(2)	23
28 U.S.C. § 2342(1)	3
28 U.S.C. § 2344	3

Communications Act of 1934, *as amended*, 47 U.S.C. §§ 151 *et seq.*:

Sec. 1, 47 U.S.C. § 151	7, 45, 46
Sec. 4(i), 47 U.S.C. § 154(i)	5, 11, 46
Sec. 229, 47 U.S.C. § 229	11
Sec. 229(a)–(b), 47 U.S.C. § 229(a)–(b)	8
Sec. 301, 47 U.S.C. § 301	5
* Sec. 302, 47 U.S.C. § 302a	5, 11, 15, 25, 41–45
Sec. 302(a), 47 U.S.C. § 302a(a).....	5, 42–43
Sec. 302(b), 47 U.S.C. § 302a(b).....	5

TABLE OF AUTHORITIES (continued)

		Page(s)
*	Sec. 303, 47 U.S.C. § 303	5, 26, 15, 43, 45–46
	Sec. 303(e), 47 U.S.C. § 303(e)	5, 26, 43, 46
	Sec. 303(g), 47 U.S.C. § 303(g)	5, 25, 45–46
	Sec. 303(r), 47 U.S.C. § 303(r)	5, 25, 46
	Sec. 312(a)(2), 47 U.S.C. § 312(a)(2)	44
	Sec. 402(a), 47 U.S.C. § 402(a)	3
	Secure and Trusted Communications Networks Act of 2019 (Secure Networks Act), Pub. L. No. 116-124, 134 Stat. 158 (2020)..... 9–11, 48, 50–51	
	Sec. 2, 47 U.S.C. § 1601	9
	Sec. 2(b)(1), 47 U.S.C. § 1601(b)(1)	32
	Sec. 3(a)(1), 47 U.S.C. § 1602(a)(1)	10
	Sec. 4, 47 U.S.C. § 1603	10
	Communications Assistance for Law Enforcement Act (CALEA), Pub. L. No. 103-414, 108 Stat. 4279 (1994)..... 8, 11, 15, 26, 47	
	Sec. 103, 47 U.S.C. § 1002	8
*	Sec. 105, 47 U.S.C. § 1004	8, 11, 47–48
	Sec. 106, 47 U.S.C. § 1005	8
	Sec. 301, 47 U.S.C. § 229	8, 11
*	Secure Equipment Act of 2021, Pub. L. No. 117-55, 135 Stat. 423..... 3, 13–17, 24–26, 31–33, 36–41, 48–51	

TABLE OF AUTHORITIES **(continued)**

	Page(s)
Sec. 2(a)(1).....	13
* Sec. 2(a)(2).....	13, 14, 32, 38
* Sec. 2(a)(3).....	13, 15, 37–38
Sec. 2(a)(3)(A).....	13, 37
Sec. 2(a)(3)(B).....	13, 16, 37
47 C.F.R. § 0.181	7
47 C.F.R. § 1.4(b)(1).....	3
47 C.F.R. §§ 1.50000–1.50003	9
47 C.F.R. § 2.803	6
47 C.F.R. §§ 2.901 <i>et seq.</i>	6
47 C.F.R. § 2.901(a)	6, 46
47 C.F.R. § 2.939(a)(4).....	32, 44
47 C.F.R. § 2.939(a)–(b) (2021).....	12
47 C.F.R. § 2.939(a)(4) (2021).....	15, 25, 37
47 C.F.R. § 2.939(e)	18, 20
47 C.F.R. § 2.939(e)(1)	19, 22
47 C.F.R. § 2.939(e)(2)	19
47 C.F.R. § 2.939(e)(3)	19, 28
47 C.F.R. § 2.939(e)(4)	20
47 C.F.R. §§ 2.1203–2.1204.....	6

TABLE OF AUTHORITIES
(continued)

Page(s)

Fed. R. App. P. 40(b)(1) 35

D.C. Cir. R. 28(a)(7) 22, 27

Other Authorities:

* H.R. Rep. No. 117-148 (2021) 10, 14, 39

GLOSSARY

2021 NPRM	<i>Protecting Against Nat'l Sec. Threats Through the Equip. Authorization Program</i> , 36 FCC Rcd. 10578 (2021), reprinted at JA____–____
2022 Order	<i>Protecting Against Nat'l Sec. Threats Through the Equip. Authorization Program</i> , 37 FCC Rcd. 13493 (2022), reprinted at JA____–____
2025 Order	<i>Protecting Against Nat'l Sec. Threats Through the Equip. Authorization Program</i> , FCC 25-71, 40 FCC Rcd. --- (rel. Oct. 29, 2025), reprinted at JA____–____
CALEA	Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994)
FCC or Commission	Respondent Federal Communications Commission
Hikvision	Hangzhou Hikvision Digital Technology Company and its subsidiaries or affiliates, including Petitioner Hikvision USA, Inc.
<i>Hikvision I</i>	<i>Hikvision USA, Inc. v. FCC</i> , 97 F.4th 938 (D.C. Cir. 2024)
Secure Equipment Act	Secure Equipment Act of 2021, Pub. L. No. 117-55, 135 Stat. 423 (codified as Note to 47 U.S.C. § 1601)
Secure Networks Act	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. §§ 1601–1608)

No. 25-1274

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

HIKVISION USA, INC.,
Petitioner,

v.

FEDERAL COMMUNICATIONS COMMISSION
and UNITED STATES OF AMERICA,
Respondents.

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

BRIEF FOR RESPONDENTS

INTRODUCTION

Two years ago, in *Hikvision USA, Inc. v. FCC*, 97 F.4th 938 (D.C. Cir. 2024) (*Hikvision I*), this Court upheld communications-equipment authorization rules that “prohibit[] the authorization of [Hikvision]’s equipment for sale and marketing in the United States * * * in the physical security surveillance of critical infrastructure,” *id.* at 950, based on the government’s determination that Hikvision’s equipment poses an unacceptable risk to national security, *see id.* at 940–43.

Following that decision, the Federal Communications Commission adopted several updates to the equipment authorization rules. *Protecting Against Nat'l Sec. Threats Through the Equip. Authorization Program*, FCC 25-71, 40 FCC Rcd. --- (rel. Oct. 29, 2025) (*2025 Order*), reprinted at JA____–____. As relevant here, those updates create a process through which the agency can review, and potentially limit, existing authorizations of equipment that would no longer be eligible to receive authorizations today due to unacceptable national security risks.

Undeterred by the Court's prior decision, Hikvision seeks to mount another facial attack on the equipment authorization rules. Its sole contention in this case is that the FCC lacks authority to consider national security risks when making equipment authorization decisions, and that such decisions must instead be based exclusively on radiofrequency interference considerations.

Hikvision has not met its burden to establish standing to press that facial challenge in this case, because it has not demonstrated any concrete and impending injury from the adoption of the rule at issue here. The challenged rule does not require or forbid any action by Hikvision, and does not itself resolve (without further proceedings) whether any limits will ultimately be imposed on the company's authorizations.

Even if Hikvision has standing, its arguments are foreclosed by the Court's decision in *Hikvision I*, which rejected Hikvision's prior challenge to rules prohibiting equipment authorization on national security grounds. In any event, Hikvision's arguments are meritless, particularly in view of the Secure Equipment Act, which ratifies and confirms the Commission's authority to refuse equipment authorizations based on an unacceptable risk to national security.

JURISDICTIONAL STATEMENT

This Court generally has jurisdiction to review final orders of the Commission under 28 U.S.C. § 2342(1) and 47 U.S.C. § 402(a). A summary of the *2025 Order* was published in the Federal Register on November 25, 2025. 90 Fed. Reg. 53227. Hikvision filed its petition for review on December 3, within 60 days of publication. *See* 28 U.S.C. § 2344; 47 C.F.R. § 1.4(b)(1). The Court lacks jurisdiction here, however, because the challenged rule does not limit Hikvision's authorizations or determine whether any limits might ultimately be imposed, and so Hikvision has not shown that it faced any concrete and impending injury (as is required for Article III standing) when it initiated this appeal. *See infra* Part I.

STATEMENT OF THE ISSUES

1. Whether Hikvision has established standing to pursue its facial challenge to a rule that creates a process through which the Commission may later limit importation and sales of covered equipment, when that rule does not require or forbid any action by Hikvision and does not itself resolve (without further proceedings) whether any limits will ultimately be imposed.

2. Whether, when deciding whether to restrict the sale or importation of communications equipment, the FCC may consider findings that the equipment poses an unacceptable risk to national security.

PERTINENT STATUTES AND REGULATIONS

Pertinent statutes and regulations are set forth in the statutory addendum bound with this brief.

STATEMENT OF THE CASE

A. Foundational Mandates Of The Commission

1. Title III of the Communications Act of 1934, as amended, “endow[s] the Commission with ‘expansive powers’ and a ‘comprehensive mandate’” to regulate radio communication in the public interest. *Cellco P’ship v. FCC*, 700 F.3d 534, 542 (D.C. Cir. 2012); see 47 U.S.C. §§ 301 et

seq. That broad authority begins with Section 301 of the Act, which sets forth Congress’s purpose “to maintain the control of the United States over all the channels of radio transmission; and to provide for the use of such channels * * * under licenses granted by Federal authority.” 47 U.S.C. § 301.

To that end, in Section 302 of the Act, Congress empowered the Commission, “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.” 47 U.S.C. § 302a(a); *see also id.* § 303(e) (similar). “No person shall manufacture, import, sell, offer for sale, or ship devices * * * which fail to comply with” the Commission’s equipment authorization rules. *Id.* § 302a(b).

Section 303(g) likewise directs the Commission, “as public convenience, interest, or necessity requires,” to “generally encourage the larger and more effective use of radio in the public interest.” 47 U.S.C. § 303(g). To accomplish this, Section 303(r) grants the Commission authority to “[m]ake such rules and regulations and prescribe such restrictions and conditions * * * as may be necessary to carry out” its mission. *Id.* § 303(r); *accord id.* § 154(i) (“The Commission may perform

any and all acts, make such rules and regulations, and issue such orders * * * as may be necessary in the execution of its functions.”).

Pursuant to this broad authority, “[i]n order to carry out its responsibilities under the Communications Act and * * * to promote the efficient use of radio spectrum, the Commission has developed technical standards and other requirements for radio frequency equipment and parts or components thereof.” 47 C.F.R. § 2.901(a). Those requirements are found in Part 2, Subpart J of the Commission’s rules, 47 C.F.R. §§ 2.901 *et seq.*, and include the provisions at issue in this case. With limited exceptions, no radiofrequency device may be sold or imported into the United States unless it complies with these equipment authorization rules. *See id.* §§ 2.803, 2.1203–2.1204.

2. Since the FCC’s creation in 1934, “[o]ne of the principal purposes” of the agency has been to help safeguard national security. *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) (discussing “the kind of national security authority [the FCC] has exercised for decades”). Indeed, in the very first sentence of the Communications Act, Congress directed the Commission to use its regulatory authority to, among other things, serve “the national defense”

and “promot[e] the safety of life and property.” 47 U.S.C. § 151. And for more than 60 years, the Commission has designated a Defense Commissioner to “direct[] the homeland security, national security and emergency preparedness, and defense activities of the Commission.” 47 C.F.R. § 0.181.

For example, the Commission has “a longstanding practice” of “assess[ing] national security and other concerns” arising from foreign ownership in the communications sector. *China Telecom*, 57 F.4th at 261; *see Huawei*, 2 F.4th at 440 (“[I]n the late 1990s, the FCC recommitted to considering ‘national security’ and ‘foreign policy’ concerns * * * that would inform its ‘public interest’ analysis”); *Rules & Pol’ys on Foreign Participation in the U.S. Telecomms. Mkt.*, 12 FCC Rcd. 23891, 23919–21 ¶¶ 61–66 (1997). In 2020, the Commission codified its practice of coordinating and consulting with other executive branch agencies on an array of FCC matters to assess national security, foreign policy, and law enforcement concerns. *Process Reform for Exec. Branch Review of Certain FCC Appls. & Pets.*, 35 FCC Rcd. 10927 (2020). And those agencies have in turn established a formal body to inform and advise the Commission on these matters. *See* Executive Order No. 13913, 85 Fed. Reg. 19643 (Apr. 4, 2020).

The FCC also plays a vital national security role in administering the Communications Assistance for Law Enforcement Act (CALEA), Pub. L. No. 103-414, 108 Stat. 4279 (1994). CALEA requires, among other things, that telecommunications carriers and equipment manufacturers comply with court orders authorizing a wiretap or law enforcement access to call records, 47 U.S.C. §§ 1002, 1005, and that carriers prevent any unlawful interception of calls or access to records, *id.* § 1004. The statute also directs the Commission to prescribe implementing rules to administer and enforce these requirements. *Id.* § 229(a)–(b).

Consistent with the FCC’s national security responsibilities, both this Court and other courts have repeatedly upheld FCC national security actions. *See Huawei, supra*, 2 F.4th 421; *China Telecom, supra*, 57 F.4th 256; *Pac. Networks Corp. v. FCC*, 77 F.4th 1160 (D.C. Cir. 2023); *China Unicom (Ams.) Ops. Ltd. v. FCC*, 124 F.4th 1128 (9th Cir. 2024); *Hikvision I, supra*, 97 F.4th 938.

B. The Secure Networks Act And The Covered List

In November 2019, the FCC adopted rules restricting federal support for communications equipment or services produced by companies that pose a national security threat to U.S. communications networks or the communications supply chain. *Protecting Against Nat’l*

Sec. Threats to the Commc'ns Supply Chain, 34 FCC Rcd. 11423 (2019). Those rules were upheld in *Huawei, supra*, 2 F.4th 421. In its ruling, the Fifth Circuit recognized that “[a]ssessing security risks to telecom networks falls in the FCC’s wheelhouse” and held that the agency had “reasonably acted within the broad authority Congress gave it to regulate communications.” *Id.* at 427.

Following the adoption of those rules, Congress codified substantially similar requirements in the Secure and Trusted Communications Networks Act of 2019 (“Secure Networks Act”), Pub. L. No. 116-124, 134 Stat. 158 (2020) (codified as amended at 47 U.S.C. §§ 1601–1608). The Secure Networks Act established a “Covered List” of equipment and services that have been determined to “pose[] an unacceptable risk to the national security of the United States or the security and safety of United States persons.” *Id.* § 1601; *see* 47 C.F.R. §§ 1.50000–1.50003. Among the equipment that Congress designated to be included on the Covered List is certain video surveillance and telecommunications equipment produced by Hikvision, the Petitioner here. *See Hikvision I*, 97 F.4th at 940–42, 944–48.

The Secure Networks Act prohibited federal funds administered by the Commission from being used to obtain or maintain equipment or

services on the Covered List. 47 U.S.C. § 1602(a)(1). It also authorized the Commission to establish a program to reimburse communications providers for the cost of removing and replacing covered equipment. *Id.* § 1603.

C. The 2021 NPRM And The Secure Equipment Act

1. In June 2021, the Commission issued a Notice of Proposed Rulemaking proposing to prohibit equipment authorization for any equipment included on the Covered List. *Protecting Against Nat’l Sec. Threats Through the Equip. Authorization Program*, 36 FCC Rcd. 10578 (2021) (*2021 NPRM*), reprinted at JA____–____. The *2021 NPRM* observed that this equipment “has been found to pose an unacceptable risk to the national security of the United States or to the security and safety of United States persons.” *Id.* ¶ 3 (JA____). Yet the Commission’s then-existing rules allowed covered equipment to be imported and sold so long as it was purchased without federal subsidies. *See* H.R. Rep. No. 117-148, at 2–3 (2021). The Commission found that “ensur[ing] that [its] rules under the Secure Networks Act effectively preclude use of equipment on the Covered List” would “serve the public interest by addressing significant national security risks.” *2021 NPRM* ¶ 65 (JA____).

The *2021 NPRM* identified authority for the Commission’s proposal in several provisions of the Communications Act. *See id.* ¶¶ 65–69 (JA____–____). The Commission first explained that the proposed restriction on equipment authorization would serve the public interest under Sections 302 and 303, as “it would appear to be in the public interest not to approve devices capable of emitting RF energy * * * if such equipment has been deemed, pursuant to law, to pose an unacceptable risk to the national security of the United States.” *Id.* ¶¶ 66–67 (JA____); *see also id.* ¶ 69 (JA____). It further recognized that a “rule prohibiting the use of equipment produced or provided by any company posing a national security threat [could] implement[]” provisions of CALEA, including the requirement to prevent unlawful access to communications and call records. *Id.* ¶ 68 (JA____–____) (citing 47 U.S.C. §§ 229 and 1004). And, invoking 47 U.S.C. § 154(i), it reasoned that the proposed rule would be “reasonably necessary to the effective enforcement of the Secure Networks Act.” *Id.* ¶ 69 (JA____); *see id.* ¶ 65 (JA____) (the proposed rule “can and should also serve the purpose of fulfilling other Commission responsibilities under the Secure Networks Act”).

2. The *2021 NPRM* also sought comment on “whether the Commission could or should revoke any existing equipment

authorizations of such ‘covered’ communications equipment, and if so, the processes for doing so.” *Id.* ¶ 80 (JA___); *see id.* ¶¶ 80–89 (JA___–___). It observed that an existing Commission rule, 47 C.F.R. § 2.939(a)–(b) (2021), already permitted equipment authorizations to be revoked in certain circumstances. *See ibid.* As it then existed, however, the rule required certain procedures that the Commission recognized might not be necessary or appropriate for covered equipment. *See id.* ¶ 87 (JA___–___).

In addition, cognizant that revocation under the existing rule could potentially make it unlawful for consumers to continue using their existing equipment, the Commission sought comment on what “outreach efforts” might be needed “to inform the public regarding any such revocations” and any “appropriate and reasonable transition period for removing that particular equipment.” *Id.* ¶ 88 (JA___); *see also id.* ¶ 87 (JA___).

Though the Commission broadly sought comment on various issues pertaining to revocation, the 2021 *NPRM* did not propose specific rules or amendments on that subject. *See id.* App’x A (JA___–___) (Proposed Rules).

3. While the *2021 NPRM* was pending, Congress enacted the Secure Equipment Act of 2021, Pub. L. No. 117-55, 135 Stat. 423 (codified as Note to 47 U.S.C. § 1601). Section 2(a)(1) of that Act—which references the *2021 NPRM* by name and docket number—directed the Commission to adopt final rules within one year. *Id.* § 2(a)(1). And Section 2(a)(2) required those rules to provide, as the *2021 NPRM* had proposed, that the Commission would “no longer review or approve any application for equipment authorization for equipment that is on the list of covered communications equipment.” *Id.* § 2(a)(2).

Section 2(a)(3) of the Secure Equipment Act addressed the issue of revocation. Under Subparagraph (A), Congress directed the Commission, when acting on the *2021 NPRM*, to not yet adopt new rules governing “revocation of any equipment authorization granted before” the resulting order. *Id.* § 2(a)(3)(A). In Subparagraph (B), however, Congress made clear that the Commission would remain free, in a subsequent rulemaking, to “adopt[] rules providing for” the “revocation of any equipment authorization on the basis of the equipment being on” the Covered List. *Id.* § 2(a)(3)(B). In other words, as reflected in the contemporaneous House Report, the Secure Equipment Act “prohibit[ed] the FCC from revoking previously issued authorizations as part of the

relevant rulemaking proceeding [then underway], but [it] does not prohibit the FCC from acting in a separate proceeding to take such action.” H.R. Rep. No. 117-148, at 5 (2021).

D. The 2022 Order And *Hikvision I*

1. The Commission completed the rulemaking referenced in the Secure Equipment Act in November 2022. *Protecting Against Nat’l Sec. Threats Through the Equip. Authorization Program*, 37 FCC Rcd. 13493 (2022) (*2022 Order*), reprinted at JA____–____. Consistent with the *2021 NPRM*’s proposal and Section 2(a)(2) of the Secure Equipment Act, the *2022 Order* updated the equipment authorization rules to prohibit authorization of equipment that has been added to the Covered List because it poses an unacceptable risk to national security. *See id.* ¶¶ 44–100 (JA____–____).

The Commission explained that it had ample legal authority to prohibit authorization of equipment posing a national security threat “on two grounds.” *Id.* ¶ 38 (JA____); *see id.* ¶¶ 38–43 (JA____–____). First, the Secure Equipment Act clearly established the Commission’s “authority to adopt rules that prohibit * * * approval of * * * equipment that is listed on the Commission’s Covered List.” *Id.* ¶ 39 (JA____). Indeed, Section 2(a)(2) of the Secure Equipment Act expressly required it to do so.

Second, the Commission affirmed the *2021 NPRM*'s conclusion that the agency's preexisting legal authority—including Section 302, Section 303, CALEA, and the agency's express statutory mission to serve “the national defense” and “promot[e] the safety of life and property”—also amply supported its actions. *Id.* ¶¶ 40–43 (JA____–____). The Commission observed that this reading of its preexisting authority “is confirmed by Congress's enactment of the Secure Equipment Act,” which identified the *2021 NPRM* by name and docket number, directed the Commission to adopt rules consistent with its proposal, and thus “clearly intended to ratify the Commission's tentative conclusions in the *NPRM* that it had authority as discussed therein.” *Id.* ¶ 42 (JA____).

3. In accordance with Section 2(a)(3) of the Secure Equipment Act, the *2022 Order* did not adopt any new rules addressing potential revocation of previously granted authorizations. The Commission observed, however, that its existing rules provided for revocation of prior authorizations “[b]ecause of conditions coming to the attention of the Commission which would warrant it in refusing to grant an original application.” 47 C.F.R. § 2.939(a)(4) (2021); *see 2022 Order* ¶¶ 103, 114 (JA____, ____). And it concluded, consistent with that rule, that the Commission “has the requisite authority under the Communications Act”

to revoke existing authorizations for covered equipment that has been found to pose an unacceptable risk to national security. *2022 Order* ¶ 114 (JA__); *see id.* ¶¶ 114–118 (JA__–__). In particular, the Commission recognized, its “authority to revoke” existing authorizations based on unacceptable risks to national security “is confirmed by the Secure Equipment Act.” *Id.* ¶ 115 (JA__). Under Section 2(a)(3)(B), the Commission explained, the agency has “discretion” in an appropriate rulemaking “to decide whether to take equipment authorization action regarding authorizations [previously] granted.” *Id.* (JA__).

Consistent with that understanding, the Commission adopted an accompanying Further Notice of Proposed Rulemaking (FNPRM) in which it began a new rulemaking proceeding and sought further comment on (among other things) whether and how to consider revoking existing authorizations for equipment on the Covered List. *See 2022 Order* ¶¶ 288–307 (JA__–__). In particular, the Commission sought comment on what situations might or might not warrant revocation and the associated costs and benefits. *Id.* ¶¶ 291–295 (JA__–__). The Commission also sought comment on whether such action should be “partial and limited”—such as by restricting only further importation and sales (but not continued use) of such equipment—or instead should

require complete revocation, and on any “appropriate and reasonable transition period.” *Id.* ¶ 296 (JA___); *see id.* ¶¶ 296–302 (JA___–___). And the Commission sought comment on whether it should update its existing rules to provide more tailored procedures for evaluating whether to revoke previously granted authorizations. *Id.* ¶¶ 303–304 (JA___).

3. Hikvision sought review of the *2022 Order* in this Court, which upheld the order in relevant part in *Hikvision I, supra*, 97 F.4th 938. As the Court explained, the challenged “ban” on “equipment authorizations for ‘covered’ equipment”—“including video surveillance and telecommunications equipment manufactured by Petitioner[] Hikvision”—was “mandated by Congress in” the Secure Equipment Act. *Id.* at 943. The Court observed that the Secure Equipment Act, after referencing the *2021 NPRM* by name and docket number, “required the Commission to ‘no longer review or approve any application for equipment authorization for equipment that is on the [Covered List].’” *Id.* at 942. The Secure Equipment Act thus “remove[d] any doubt that the FCC was empowered to issue the equipment-authorization ban” that Hikvision challenged. *Id.* at 945; *see id.* at 948 (“Congress has ‘power to ratify the acts which it might have authorized’”) (quoting *United States v. Heinszen*, 206 U.S. 370, 384 (1907)). The Court therefore “uph[e]ld the FCC’s Order to the

extent that it prohibits the authorization of [covered] equipment.” *Id.* at 950. (In a separate portion of the decision that is not at issue here, the Court vacated and remanded the *2022 Order*’s definition of “critical infrastructure.” *See id.* at 948–50.)

E. The *2025 Order* Under Review

In the *2025 Order* now at issue, the Commission adopted several incremental updates, “[b]uilding on the record received” in response to the FNPRM, the Commission’s “experience implementing the prohibition” adopted in the *2022 Order*, “and other recent Commission actions aimed at protecting our nation’s communications networks and supply chain.” *2025 Order* ¶ 1 (JA____).

Hikvision challenges only one aspect of the *2025 Order*: an amendment to the equipment authorization rules creating “a procedure whereby the Commission can limit previously granted authorizations of covered equipment to prohibit the[ir] continued importation and marketing, without prohibiting the continued use of such devices.” *2025 Order* ¶ 40 (JA____); *see id.* ¶¶ 32–50 (JA____–__); 47 C.F.R. § 2.939(e) (JA____–__). Although this amended rule arose from the Commission’s earlier requests for comment on whether to revoke existing authorizations for equipment now included on the Covered List, *see 2025 Order* ¶¶ 33–

39 (JA____–__), it is narrower than earlier proposals in two important respects.

First, under the rule adopted here, restricting existing authorizations for covered equipment is neither automatic nor mandatory. Instead, if considering action under the rule, Commission staff must “issue a public notice” and “provide for a public comment period of no less than 30 days.” 47 C.F.R. § 2.939(e)(1) & (3) (JA____). “The public notice will include an [initial] assessment * * * of public interest factors,” including “risks the equipment [may] pose” and “the economic and supply chain impacts” if the authorization were to be limited. *Id.* § 2.939(e)(2) (JA____); *see 2025 Order* ¶ 44 (JA____–__). The agency “may consider such countervailing economic concerns” and “could conclude that [these] other factors outweigh any national security risks.” *2025 Order* ¶ 46 (JA____–__); *see also id.* ¶ 50 (JA____) (staff must “fully consider[] the ramifications” both “with regard to the [regulated] party” and to “the public at large,” and must “balanc[e] the public interest factors regarding the supply chain and consumer interests”). Commission staff must therefore “review the submissions” received and “may request additional information as may be appropriate” before making an official “determination as to whether to place limitations on the existing authorization * * *, providing the

reasons for such decision.” 47 C.F.R. § 2.939(e)(4) (JA____); *see 2025 Order* ¶ 47 (JA____).

Second, in contrast to complete revocation, the rule adopted here does not restrict consumers’ continued use of equipment they have previously purchased. The rule permits the agency to “limit[] * * * an existing authorization for covered equipment authorizations to prohibit continued importation or marketing,” 47 C.F.R. § 2.939(e) (JA____), but does “not affect consumers’ continued use or operation of devices they already possess,” *2025 Order* ¶ 40 (JA____). This approach “limit[s] the scope of an existing authorization * * * to prohibit continued importation or marketing * * * without revoking the underlying authorization,” *id.* ¶ 42 (JA____), and “reduces the challenges that commenters suggested would arise” if the Commission were to “engage in revocations that also prohibit the use or operation of such covered equipment,” *id.* ¶ 50 (JA____).*

* Hikvision notes (Br. 14) that several commenters opposed revocation of existing authorizations. Some of the same commenters also indicated, though, that they could support “some form of prospective approach to revocation of covered equipment that would prohibit [its] future marketing or sale” without restricting continued operation or use of equipment previously purchased. *2025 Order* ¶ 39 (JA____);
(cont’d)

The Commission thus adopted “a simplified, prospective approach” compared to earlier proposals, *id.* ¶ 40 (JA____), that it deemed “well-tailored to address unacceptable national security risks without disrupting continued use or operation of devices,” *id.* ¶ 41 (JA____). Referencing its prior analysis in the *2022 Order*, *see id.*, and “[c]onsistent with [its] existing regulatory procedures,” *id.* ¶ 42 (JA____), the Commission explained that the agency “has the requisite authority * * * to limit the scope of an existing authorization” to “protect[] American communications networks from devices specifically determined to ‘pose an unacceptable risk to the national security of the United States,’” *ibid.*; *see id.* ¶ 33 & n.123 (JA____) (citing the *2022 Order*); *id.* ¶ 42 n.178 (JA____) (“The adoption of this new procedure is consistent with our existing authority to revoke equipment authorizations”).

see, e.g., CTIA Comments at 15 (JA____). Other commenters voiced strong support for revoking or limiting previously granted authorizations for equipment now included on the Covered List. *2025 Order* ¶¶ 38, 43 (JA____, ____); *see* Found. for Def. of Democracy Letter at 1–3 (JA____–__); Heritage Found. Letter at 3 (JA____); Horizon Advisory Letter at 5 (JA____); Hudson Inst. Letter at 4 (JA____); Motorola Comments (JA____–__).

F. Subsequent Developments

Hikvision filed its petition for review of the *2025 Order* on December 3. Months later, on March 27, the FCC’s Public Safety and Homeland Security Bureau and its Office of Engineering and Technology issued a Public Notice under 47 C.F.R. § 2.939(e)(1) proposing to limit the importation and marketing of any previously authorized equipment that was added to the Covered List in 2024 or earlier. Public Notice, DA 26-294, 2026 WL 1013687 (Mar. 27, 2026), <https://perma.cc/E34R-H2U9>. A summary of the Public Notice was published in the Federal Register on April 6, and public comments are due on or before May 6. 91 Fed. Reg. 17275 (Apr. 6, 2026).

STANDARD OF REVIEW

As the Petitioner, Hikvision bears the burden of establishing that it has standing in this case. *Entergy Ark., LLC v. FERC*, 134 F.4th 576, 580, 583–84 (D.C. Cir. 2025). “[Like] a plaintiff moving for summary judgment,” Hikvision “must support each element of its claim to standing by affidavit or other evidence” and must “show a substantial probability that” each element is satisfied. *Sierra Club v. EPA*, 292 F.3d 895, 899 (D.C. Cir. 2002) (internal quotation marks omitted); see D.C. Cir. R. 28(a)(7).

Under the Administrative Procedure Act, a court may not overturn agency action unless it is arbitrary, capricious, or otherwise contrary to law. *See* 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 (Ams.) v. FCC*, 57 F.4th 256, 264 (D.C. Cir. 2022) (quoting *FCC v. Prometheus Radio Project*, 592 U.S. 414, 423 (2021)).

On matters of statutory interpretation, “[c]ourts must exercise their independent judgment in deciding whether an agency has acted within its statutory authority.” *Loper Bright Enters. v. Raimondo*, 603 U.S. 369, 412 (2024). “In exercising such judgment, though,” courts may appropriately “seek aid from the interpretations of” the implementing agency. *Id.* at 394; *see also id.* at 412–13. Courts are especially respectful of agencies’ views on “[m]atters intimately related to foreign policy and national security,” which “are rarely proper subjects for judicial intervention.” *China Telecom*, 57 F.4th at 267 (quoting *Haig v. Agee*, 453 U.S. 280, 292 (1981)).

SUMMARY OF THE ARGUMENT

I. Hikvision has not met its burden to establish standing to pursue this facial challenge because it has not shown that it faced any concrete and impending injury when it initiated this appeal. The challenged rule does not require or forbid any action by Hikvision, nor does the rule itself determine (without further proceedings) whether any limits will ultimately be imposed on Hikvision's authorizations. Hikvision's vague assertions that unspecified customers might be reducing or postponing purchases of Hikvision equipment because of the rule—and not for other reasons—are unsubstantiated and implausible.

II. Even if Hikvision has standing, its challenge to the Commission's authority to consider and address national security risks fails on the merits.

A. The Secure Equipment Act conclusively establishes that the Commission may consider national security concerns when deciding whether to grant equipment authorizations. It thereby forecloses Hikvision's contention that the Commission lacks such authority and that such decisions must instead be based exclusively on radiofrequency interference considerations. There is no sound basis for treating the rule at issue here, which creates a process to review and potentially limit

previously granted authorizations based on national security risks, differently from the rules already upheld in *Hikvision I*, which prohibit new authorizations for covered equipment based on the same national security risks. Indeed, Congress passed the Secure Equipment Act against the backdrop of an existing regulation providing that “[t]he Commission may revoke any equipment authorization * * * [b]ecause of conditions coming to the attention of the Commission which would warrant it in refusing to grant an original application.” 47 C.F.R. § 2.939(a)(4) (2021). And Section 2(a)(3)(B) of the Secure Equipment Act specifically contemplates that the Commission may, in an appropriate rulemaking, “adopt[] rules providing for” the “review or revocation of any equipment authorization on the basis of the equipment being on the” Covered List—which is precisely what the Commission did here.

B. Although the Court need not reach the issue, the FCC’s preexisting Title III authority already provided ample support for its equipment authorization rules. Section 302 of the Communications Act authorizes the Commission to adopt reasonable regulations governing devices that emit radiofrequency energy capable of interfering with radio communications, consistent with the public interest. This authority is buttressed by Sections 303(g) and 303(r), which empower the

Commission to adopt rules and regulations to promote the larger and more effective use of radio in the public interest, as it would be neither an efficient nor an effective use of radio spectrum to authorize radiofrequency devices that pose an unacceptable risk to national security. And Section 303(e) specifies that the Commission may “[r]egulate the kind of apparatus to be used” not only as to “the purity and sharpness of the emissions” but also as to “external effects” more broadly, which readily encompasses national security-related effects. The challenged rule also finds support in CALEA, because prohibiting the importation and sale of unsafe equipment enables carriers to prevent unlawful interception of calls or access to call records. These provisions collectively supply ample authority to address national security risks when making equipment authorization decisions. That authority has now been ratified and reinforced by the Secure Equipment Act, which shows that Congress approved of the Commission’s actions.

ARGUMENT

I. HIKVISION HAS NOT ESTABLISHED STANDING TO PURSUE ITS FACIAL CHALLENGE.

Hikvision has not met its burden to establish standing to pursue its facial challenge to the *2025 Order*. To satisfy “the irreducible

constitutional minimum of standing,” Hikvision must first demonstrate an “injury in fact”—that is, an injury that is “(a) concrete and particularized, and (b) actual or imminent, not conjectural or hypothetical.” *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992) (citations and internal quotation marks omitted). It must then further show causation, meaning that the injury is “fairly traceable to the challenged action,” and redressability, requiring that it is “likely * * * that the injury will be redressed by a favorable decision.” *Id.* at 560–61 (alterations and internal quotation marks omitted).

As the Petitioner, Hikvision bears the “burden of proof * * * to show a ‘substantial probability’” for each element of standing. *Sierra Club v. EPA*, 292 F.3d 895, 899 (D.C. Cir. 2002). And it “must make this evidentiary presentation * * * no later than when it files its opening brief.” *Entergy Ark., LLC v. FERC*, 134 F.4th 576, 581 (D.C. Cir. 2025) (quoting *Twin Rivers Paper Co. v. SEC*, 934 F.3d 607, 613 (D.C. Cir. 2019)); *see id.* at 580–83; D.C. Cir. R. 28(a)(7).

1. Hikvision’s first theory to support standing (Br. 21) is that the company is “the object of the agency action under review.” But the rule Hikvision challenges does not itself “require or forbid [any] action by” Hikvision. *FDA v. All. for Hippocratic Medicine*, 602 U.S. 367, 382

(2024); *see, e.g., Saline Parents v. Garland*, 88 F.4th 298, 307–08 (D.C. Cir. 2023) (pre-enforcement challenge not reviewable when challenged documents did not “require[]” the appellant “to engage in, or to refrain from, any conduct”). Before any existing authorizations may be limited under the rule, Commission staff must await public comment, thoroughly review the costs and benefits of restricting any authorizations, and balance the full array of public interest considerations to decide whether and how to proceed. *See* 47 C.F.R. § 2.939(e)(3) (JA____–__); *2025 Order* ¶¶ 44–50 (JA____–__). Hikvision’s standing to challenge the rule at this juncture is thus subject to “contingencies” that make it ill-suited for a pre-enforcement facial challenge. *Saline Parents*, 88 F.4th at 306 (quoting *Trump v. New York*, 592 U.S. 125, 131 (2020) (per curiam)).

Hikvision’s lack of standing is not cured by the subsequent Public Notice initiating that further examination and proposing to limit previously granted authorizations, nor by any potential future action adopting such limits. That is because standing must exist “at the time the petition challenging the rule was filed.” *Am. Petrol. Inst. v. U.S. EPA*, 216 F.3d 50, 64 & n.3 (D.C. Cir. 2000); *see, e.g., Chamber of Com. of the U.S. v. EPA*, 642 F.3d 192, 200 (D.C. Cir. 2011); *N.M. Att’y Gen. v. FERC*, 466 F.3d 120, 122 (D.C. Cir. 2006) (per curiam); *SunCom Mobile & Data*,

Inc. v. FCC, 87 F.3d 1386, 1389 (D.C. Cir. 1996); *see also Sierra Club*, 292 F.3d at 901 (a petitioner must “establish its standing at the outset of its case * * * to invoke the jurisdiction of the court”). When Hikvision filed this facial challenge to the rule, the rule itself had not caused the company any concrete injury, nor was any such injury “certainly impending.” *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 409 (2013) (quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990)).

To be sure, if the Commission proceeds with further action to limit any of Hikvision’s existing authorizations, the company may then be able to raise its arguments in an as-applied challenge. *See Functional Music, Inc. v. FCC*, 274 F.2d 543, 546–47 (D.C. Cir. 1959). But the prospect that the Commission might take such action in a subsequent proceeding does not confer standing here. Hikvision therefore has not established its standing in this appeal, filed before the agency had taken any concrete steps to potentially limit any authorizations, to pursue a facial challenge to the rule.

2. Hikvision’s separate efforts to identify a here-and-now injury also fail. Hikvision contends that the *2025 Order* “is presently causing it financial harm” (Br. 21) because, it asserts, some (unspecified) customers have postponed or suspended some (unidentified) projects “involving”

Hikvision equipment. *See* Decl. of Wu Chen ¶ 4 (Pet. Add. 1). And it vaguely claims that, “[b]eginning in late 2025,” it “observed measurable changes in customer procurement and project planning behavior” that it attributes to “perceived regulatory risk.” *Ibid.* Yet Hikvision has supplied no concrete evidence to substantiate those assertions—such as any concrete examples of customers canceling or reducing scheduled orders.

What is more, Hikvision has not shown a substantial probability that any perceived sales impact was caused by the action challenged here. Any decline in sales to U.S. customers “may [be] attributable entirely to other factors”—like Hikvision’s placement on the Covered List, the *2022 Order*’s prohibition on new equipment authorizations for covered Hikvision products, or this Court’s 2024 decision in *Hikvision I* upholding those actions—rather than the *2025 Order* under review. *See Ass’n of Flight Attendants v. U.S. DOT*, 564 F.3d 462, 465–66 (D.C. Cir. 2009). Hikvision does not present statements from any customers attributing any cancellations or reductions to the rule at issue here, or committing that they will resume any forgone purchases if this particular rule is overturned. Without concrete evidence establishing that causal link, Hikvision’s mere “assertion of causation” is insufficient. *Id.* at 466; *see Entergy Ark.*, 134 F.4th at 581 (the petitioner’s “principal brief” must

supply “a clear understanding” of “the chain of causation” from the challenged action to the asserted injury “and how a decision of this court [would] redress those harms”); *Ass’n of Flight Attendants*, 564 F.3d at 468–69 (rejecting rudimentary data analysis as failing to show a “causal[] tie”).

II. THE COMMISSION HAS AUTHORITY TO CONSIDER AND ADDRESS NATIONAL SECURITY RISKS THROUGH ITS EQUIPMENT AUTHORIZATION RULES, INCLUDING BY REVOKING OR LIMITING EXISTING AUTHORIZATIONS.

Even if Hikvision had standing, its challenges to the Commission’s authority fail on the merits. As reflected in the Court’s previous decision in *Hikvision I*, the Secure Equipment Act conclusively establishes that the Commission may consider and address national security risks in its equipment authorization rules. Congress thereby ratified and reinforced the Commission’s preexisting Title III authority.

A. The Secure Equipment Act Confirms That The Commission May Base Equipment Authorization Decisions On National Security Concerns.

1. In the Secure Equipment Act, Congress directed the FCC to amend its equipment authorization rules to prohibit authorization of equipment on the Covered List—*i.e.*, equipment that has been determined to pose an unacceptable risk to the national security of the

United States or the safety and security of U.S. persons. Secure Equipment Act § 2(a)(2), 135 Stat. at 423; *see* 47 U.S.C. § 1601(b)(1). In doing so, Congress made clear that the Commission has the authority to consider and address national security risks in its equipment authorization rules—and that the Commission in turn may limit or revoke equipment authorizations on those same grounds. *See 2025 Order* ¶ 41 (JA____) (citing the *2022 Order*); *2022 Order* ¶¶ 114–117 (JA____–__); 47 C.F.R. § 2.939(a)(4). The Secure Equipment Act thus squarely forecloses Hikvision’s contention that the Commission lacks such authority and that such decisions must instead be based exclusively on radiofrequency interference considerations.

To be sure, the Secure Equipment Act is not phrased as an explicit grant of authority to the agency. But it is well established that when Congress directs an agency to promulgate, maintain, or reinstate a rule, this operates to “amend[] the applicable substantive law” to the extent it might otherwise have made that action unlawful. *Friends of Animals v. Jewell*, 824 F.3d 1033, 1043, 1045 (D.C. Cir. 2016); *All. for the Wild Rockies v. Salazar*, 672 F.3d 1170, 1174–75 (9th Cir. 2012) (citing *Robertson v. Seattle Audubon Soc’y*, 503 U.S. 429, 437–41 (1992)).

Hikvision focuses its arguments (Br. 23–34) on its contention that the Commission’s preexisting Title III authority would not have empowered the agency to refuse equipment authorization based on national security concerns. Whatever the merits of such arguments before the Secure Equipment Act, *but see infra* Part II.B, the Secure Equipment Act now requires that this authority be read to confer that power. *See 2022 Order* ¶ 41 (JA___) (“That the Commission has such authority is confirmed by the Secure Equipment Act.”). Congress thereby clarified the proper understanding of its earlier enactments “through operation of the canon that specific provisions qualify general ones.” *Robertson*, 503 U.S. at 440.

2. The same conclusion necessarily follows from the Court’s decision in *Hikvision I*, which upheld rules prohibiting authorization of covered equipment by entities that pose an unacceptable risk to national security. *See* 97 F.4th at 945 (holding that the Secure Equipment Act “remove[d] any doubt that the FCC was empowered to issue the equipment-authorization ban that [Hikvision] challenge[s]”); *id.* at 950 (“[W]e uphold the FCC’s Order to the extent that it prohibits the authorization of [Hikvision]’s equipment for sale and marketing in the

United States for use in the physical security surveillance of critical infrastructure * * *.”).

That decision is controlling here under both the law-of-the-case and law-of-the-circuit doctrines. *See LaShawn A. v. Barry*, 87 F.3d 1389 (D.C. Cir. 1996) (en banc). Though *Hikvision I* did not directly speak to the statutory authority issue, these doctrines “encompass[] a court’s explicit decisions[] as well as those issues decided by necessary implication.” *Williamsburg Wax Museum, Inc. v. Historical Figures, Inc.*, 810 F.2d 243, 250 (D.C. Cir. 1987); accord *LaShawn A.*, 87 F.3d at 1394–95; *Fogel v. Chestnutt*, 668 F.2d 100, 108–09 (2d Cir. 1981) (Friendly, J.). Because Hikvision’s view of the FCC’s statutory authority implies that the rules challenged in *Hikvision I* should not have been upheld, it is necessarily foreclosed by that decision.

Moreover, to the extent Hikvision failed to obtain a specific ruling on this issue in its prior appeal, the “well-established principles of waiver, exhaustion of remedies[,] and law of the case” make it “inappropriate to consider [it] on a second appeal following remand.” *Nw. Ind. Tel. Co. v. FCC*, 872 F.2d 465, 470 (D.C. Cir. 1989) (citing *Laffey v. Nw. Airlines*, 740 F.2d 1071, 1089–90 (D.C. Cir. 1984) (per curiam)). If Hikvision believes that it *did* properly raise the issue in its earlier appeal but the

court's decision did not fully address it, Hikvision could and should have called the court's attention to the issue by filing a petition for panel rehearing, rather than wait to raise the issue anew in a future case. *See* Fed. R. App. P. 40(b)(1) ("A petition for panel rehearing must [identify] each point of law or fact that the petitioner believes the court has overlooked or misapprehended"). In all events, Hikvision may not belatedly seek to litigate or relitigate it now. *See, e.g., Omni Outdoor Advert., Inc. v. Columbia Outdoor Advert., Inc.*, 974 F.2d 502, 505–06 (4th Cir. 1992) (addressing why raising the same arguments in a second appeal is inefficient and unfair to adversaries and the judicial system); *see also Colo. Radio Corp. v. FCC*, 118 F.2d 24, 26 (D.C. Cir. 1941) ("No judging process * * * could operate efficiently or accurately" if a party could "sit back and hope that a decision will be in its favor, and then, when it isn't, to parry with an offer of more evidence.").

3. Nor can Hikvision contend (Br. 1) that a different result should follow here than in *Hikvision I* because that case involved rules prohibiting *new* authorizations based on national security risks (which it must now concede is lawful), whereas the rule here could limit *existing* authorizations based on those same risks. That distinction fails for at least three reasons.

First, Hikvision offers no coherent statutory basis for such a distinction. Its position here is that the Commission’s authority to regulate radiofrequency equipment is limited to addressing “interference concerns” and does not encompass “purported national security issues.” See Br. 25–26, 33–35. If that position were correct, it would apply just as much to rules restricting new authorizations based on national security risks as it does to rules restricting existing authorizations based on national security risks. Because “[n]othing in the language of the statute” supports such a distinction, Hikvision’s position “ultimately proves too much.” *China Unicom (Ams.) Ops. Ltd. v. FCC*, 124 F.4th 1128, 1143–44 (9th Cir. 2024).

Second, when Congress made clear in the Secure Equipment Act that the Commission may consider national security risks when deciding whether to grant authorizations, that power “must be understood as carrying with it an implied incidental authority to revoke” such authorizations on the same basis. *China Unicom*, 124 F.4th at 1143; see *id.* at 1144–45 (discussing *Haig v. Agee*, 453 U.S. 280, 290–91 (1981)). “[C]ommon sense already suggests” that “a statutory grant of agency authority to ‘issue’ an authorization document may carry with it an

implied ancillary grant of authority to ‘deny’ and to ‘revoke’ such documents.” *Id.* at 1145.

That is especially so when Congress acted against the backdrop of an existing regulation providing that “[t]he Commission may revoke any equipment authorization * * * [b]ecause of conditions coming to the attention of the Commission which would warrant it in refusing to grant an original application.” 47 C.F.R. § 2.939(a)(4) (2021); *see Goodyear Atomic Corp. v. Miller*, 486 U.S. 174, 184–85 (1988) (courts “generally presume that Congress is knowledgeable about existing law pertinent to the legislation it enacts”); *2021 NPRM* ¶¶ 81, 85 (JA____, ___) (calling attention to the pertinent regulation).

Third, the Secure Equipment Act specifically contemplates in Section 2(a)(3)(B) that the Commission may, in a subsequent rulemaking, “adopt[] rules providing for” the “review or revocation of any equipment authorization on the basis of the equipment being on the” Covered List. Secure Equipment Act § 2(a)(3)(B), 135 Stat. at 423; *see 2022 Order* ¶¶ 115–116 (JA____–__). That is precisely what the Commission did in this rulemaking.

Hikvision observes (Br. 11) that Section 2(a)(3)(A) of the Secure Equipment Act directed the Commission not to address revocation of

existing authorizations in its initial rulemaking under the *2021 NPRM*. There may well have been good reason for Congress to have wanted the Commission to defer that issue to a subsequent rulemaking, without forbidding such future action. The *2021 NPRM* sought general comment on revocation, but did not include any specific proposed rules on that subject, and revocation raises many issues not implicated by applications for new authorizations. See *2022 Order* ¶¶ 288–305 (JA____–__) (seeking further comment on these issues); *2025 Order* ¶¶ 32–50 (JA____–__). And Section 2(a)(2) of the Secure Equipment Act required the Commission to complete its rulemaking on that NPRM within one year. Congress may sensibly have thought that the question of revoking existing authorizations would benefit from an additional and more focused round of notice and comment—and indeed, the rule ultimately adopted here as a result of that new rulemaking is considerably more nuanced than earlier proposals. Nothing in Section 2(a)(3) is reasonably understood to prevent the Commission from acting in this further proceeding.

The Commission’s action here—conducting a new rulemaking to adopt rules governing review of existing authorizations for equipment that poses unacceptable risks to national security—is precisely the

exercise of statutory authority that Congress contemplated and approved in the Secure Equipment Act. Congress “prohibit[ed] the FCC from revoking previously issued authorizations as part of the relevant [2021] rulemaking proceeding, but d[id] not prohibit the FCC from acting in a [subsequent] proceeding to take such action,” as it did here. H.R. Rep. No. 117-148, at 5 (2021).

4. Hikvision’s suggestion that the Commission disclaimed reliance on the Secure Equipment Act (Br. 20, 37–38) is unfounded. For support, Hikvision points to a footnote in the *2025 Order* stating that the rule does not “claim any new authority” because it is “consistent with our existing authority to revoke equipment authorizations.” *2025 Order* ¶ 42 n.178 (JA___). That language simply reflects that the Secure Equipment Act does not purport to be a freestanding grant of new authority, but instead embodies Congress’s authoritative construction of the Commission’s existing authority. *See supra* p. 32. Far from disclaiming any reliance on the Secure Equipment Act, the footnote correctly explains how the Secure Equipment Act supports the Commission’s actions here.

Hikvision’s contention that the Commission disavowed reliance on the Secure Equipment Act also disregards that the *2025 Order* expressly incorporates the *2022 Order*’s analysis of the Commission’s authority to

revoke existing authorizations, which construed the Secure Equipment Act in the same way we do here. *See 2025 Order* ¶ 41 (JA____); *2022 Order* ¶¶ 114–117 (JA____–__). In “conclud[ing] that * * * the Commission[] [had authority] to revoke an existing equipment authorization under” its preexisting revocation rule, the *2022 Order* explained at some length how that authority is “confirmed by the Secure Equipment Act.” *Id.* ¶¶ 114, 115 (JA____); *see id.* ¶¶ 115–117 (JA____–__). In the *2025 Order*, the Commission cited that “conclu[sion] that it has the requisite authority” from the *2022 Order* as supporting its “adopt[ion] [of] a new process” tailored to addressing existing authorizations of equipment on the Covered List. *2025 Order* ¶ 41 (JA____); *see also id.* ¶ 42 (JA____) (“Consistent with our existing regulatory procedures * * * the Commission has the requisite authority to evaluate, craft, and implement this process”).

Finally, any quarrels Hikvision might have with precisely how the Commission articulated the statutory basis for its rule are irrelevant, because the Commission’s statutory authority to adopt the rule is a pure question of law for the court and the Secure Equipment Act clearly establishes that the Commission has the requisite statutory authority. *See, e.g., Canonsburg Gen. Hosp. v. Burwell*, 807 F.3d 295, 304 (D.C. Cir.

2015) (explaining that the principle articulated in *SEC v. Chenery Corp.*, 332 U.S. 194, 196 (1947), that a court may affirm agency action solely on the grounds articulated by the agency “only limits judicial review of factual determinations or policy judgments” and “does not apply to legal principles” or “the sort of antecedent determination[s] that a court usually makes” (internal quotations marks and alterations omitted)); *see also id.* at 304–06 (collecting cases).

B. The Secure Equipment Act Ratifies And Reinforces The Commission’s Preexisting Title III Authority.

Although the Court need not reach the issue, the FCC’s preexisting Title III authority already provided ample support for its equipment authorization rules, as the Secure Equipment Act later confirmed.

1. Section 302 is reasonably read, as this Court read it in *Hikvision I*, to “authorize[] [the FCC] to regulate devices that emit radiofrequency energy that could interfere with radio communications.” 97 F.4th at 942; *cf. 2025 Order* ¶ 42 (JA____) (Section 302 “authorizes the Commission—consistent with the public interest, convenience, and necessity—to promulgate regulations applicable to * * * radiofrequency devices”). Hikvision admits that its covered equipment is “capable of emitting radiofrequency energy and thus causing interference” (Br. 4),

which brings those products within the ambit of Section 302 and the Commission's equipment authorization rules.

For devices that fall within the FCC's regulatory jurisdiction, the Commission is not limited to considering only technical concerns like interference. Rather, Section 302 broadly authorizes the Commission to adopt "reasonable" regulations "consistent with the public interest, convenience, and necessity." 47 U.S.C. § 302a(a). As the Supreme Court has explained, this language grants the Commission broad authority "so long as [its] view is based on consideration of permissible factors and is otherwise reasonable." *FCC v. WNCN Listeners Guild*, 450 U.S. 582, 593–95 (1981) (quoting *FCC v. Nat'l Citizens Comm. for Broad.*, 436 U.S. 775, 793 (1978)). And it is well established that the public interest standard permits consideration of national security risks. *See, e.g., Huawei Techs. USA, Inc. v. FCC*, 2 F.4th 421, 439–40, 443–44 (5th Cir. 2021); *China Telecom (Ams.) v. FCC*, 57 F.4th 256, 261–62 (D.C. Cir. 2022); *Pac. Networks Corp. v. FCC*, 77 F.4th 1160, 1164–65 (D.C. Cir. 2023); *China Unicom*, 124 F.4th at 1135, 1150, 1151–54.

Hikvision seeks (Br. 24–26) to place undue weight on Section 302(a)'s reference to "interference potential." That language, like the parallel reference to "emi[ssion] [of] radio frequency energy * * * in

sufficient degree to cause harmful interference,” simply identifies the class of devices to which Section 302 applies: devices that emit radiofrequency energy in sufficient amount to potentially interfere with radio communications. 47 U.S.C. § 302a(a). It does not purport to be an independent limit on the Commission’s power to adopt reasonable regulations of such devices to serve the public interest. Indeed, Hikvision’s narrow reading of Section 302 is at odds with Section 303(e), which empowers the Commission to regulate not only “the purity and sharpness of the emissions”—factors affecting interference potential—but also “external effects” more broadly. *Id.* § 303(e); *see infra* pp. 46–47.

To be sure, the FCC’s power to regulate radiofrequency devices under Section 302 is not unlimited. The agency may adopt only “reasonable” regulations that are “consistent with the public interest, convenience, and necessity.” 47 U.S.C. § 302a(a). Courts may review whether FCC regulations comply with that standard. *See* Hikvision Br. 25, 31 (describing this language as “a limitation on” the Commission’s Section 302 authority); *cf. Nat’l Broad. Co. v. United States*, 319 U.S. 190, 225–26 (1943) (rejecting claim that the “public interest” is “indefinite” or “without any standard to guide determinations”). In this case, however, there can be little question that restricting devices that pose an

unacceptable risk to national security is reasonable and in the public interest. Even Hikvision does not appear to dispute that it may be reasonable to revoke an authorization based on conditions that would have warranted denying the authorization in the first place. *Cf.* 47 U.S.C. § 312(a)(2); 47 C.F.R. § 2.939(a)(4); *see China Unicom*, 124 F.4th at 1150 (holding that the FCC may “revoke a § 214(a) certificate by invoking grounds that that it may properly consider in denying issuance of such certificate as an original matter”).

Hikvision cites (Br. 33–35) legislative history indicating that Congress’s adoption of Section 302 was motivated in large part by concerns about interference. But as the Supreme Court has recognized, Congress “often go[es] beyond the principal evil” that motivated a law and addresses an issue more broadly, “and it is ultimately the provisions of our laws rather than the principal concerns of our legislators by which we are governed.” *Nat’l Cable & Telecomms. Ass’n v. FCC*, 567 F.3d 659, 663 (D.C. Cir. 2009) (quoting *Oncale v. Sundowner Offshore Oil Servs.*, 523 U.S. 75, 79 (1998)).

Hikvision’s reliance (Br. 27–28) on *American Library Ass’n v. FCC*, 406 F.3d 689 (D.C. Cir. 2005), is misplaced. In that case, the court held that the FCC lacked authority to regulate the operation of consumer

electronics when those devices are *not* engaged in communications—there, rules governing use of digital video recorders to replay or redistribute previously recorded content. *Id.* at 691, 700, 703. That situation, the court explained, falls outside the FCC’s basic jurisdictional grant over “communication by wire and radio.” 47 U.S.C. § 151; *see Am. Libr. Ass’n*, 406 F.3d at 692 (“The Commission’s general jurisdictional grant * * * encompasses the regulation of apparatus * * * only while those apparatus are engaged in the process of” communication); *id.* at 702 (the Commission may not “assert[] jurisdiction over matters that are beyond the compass of wire or radio communications”). Here, by contrast, deciding whether to allow the importation and sale of devices that seek to engage in radiofrequency transmission (or otherwise to emit radiofrequency energy capable of causing harmful interference) falls squarely within the FCC’s regulatory jurisdiction.

2. The Commission’s Section 302 authority is buttressed by Section 303. *See 2025 Order* ¶ 31 & n.121 (JA____). Section 303(g) directs the Commission—again, “as public convenience, interest, or necessity requires”—to “generally encourage the larger and more effective use of radio in the public interest.” 47 U.S.C. § 303(g). And Section 303(r) confers associated rulemaking authority to “[m]ake such

rules and regulations and prescribe such restrictions and conditions * * * as may be necessary to carry out” the Commission’s assigned mission and responsibilities. *Id.* § 303(r); *see also id.* § 154(i). The Supreme Court has specifically held that Sections 303(g) and 303(r) “preclude the notion that the Commission is empowered to deal only with technical and engineering impediments.” *Nat’l Broad. Co.*, 319 U.S. at 217.

The Commission’s equipment authorization rules echo and invoke this statutory authority, stating that the rules have been adopted “to carry out [the Commission’s] responsibilities under the Communications Act and * * * to promote efficient use of the radio spectrum.” 47 C.F.R. § 2.901(a). After all, it would be neither an efficient nor an effective use of radio spectrum to permit radiofrequency devices that have been deemed to pose an unacceptable threat to the national security of the United States. *2021 NPRM* ¶ 67 (JA___). Nor would it serve “the purpose of the national defense” or “the purpose of promoting safety of life and property” to allow such devices. 47 U.S.C. § 151; *see Huawei*, 2 F.4th at 439; *Pac. Networks*, 77 F.4th at 1164–65.

Section 303(e) additionally empowers the Commission to regulate “the kind of apparatus to be used with respect to its external effects and the purity and sharpness of the emissions.” 47 U.S.C. § 303(e). “[E]xternal

effects” is an expansive term that can be readily understood to include national security-related effects. *See 2025 Order* ¶ 31 & n.121 (JA____). That is reinforced by the text and structure of this provision, which distinguishes the broad term “external effects” from the narrower, interference-minded phrase “purity and sharpness of the emissions.” *See United States v. Speakman*, 594 F.3d 1165, 1171 (10th Cir. 2010) (when two terms or phrases are joined by the word “and,” they are presumed to have separate meaning); *Qwest Commc’ns Int’l, Inc. v. FCC*, 398 F.3d 1222, 1236 (10th Cir. 2005) (similar).

3. As the Commission has recognized, the challenged rule also finds support in CALEA. *See 2022 Order* ¶ 41 (JA____). Section 105 of CALEA requires that telecommunications carriers “shall ensure that any interception of communications or access to call-identifying information * * * can be activated only in accordance with a court order or other lawful authorization.” 47 U.S.C. § 1004. And Section 301 of CALEA directs 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).

Hikvision observes (Br. 37) that Section 105 addresses what carriers must do to safeguard access to their networks, not what manufacturers must do. But the equipment authorization rules directly bear on carriers' ability to meet their obligations under Section 105 by prohibiting importation and sale of unsafe equipment that could be connected to the carriers' networks. *See 2022 Order* ¶ 41 (JA___) (“[T]he rules we adopt here will help ensure” that equipment connected to carriers' networks “will not include such unlawful interception capabilities[,] because use of equipment from companies that are identified * * * to pose a national security threat is far more likely to be subject to unauthorized access.”).

4. The FCC's authority to address communications-related national security threats is confirmed by established practice. As the Fifth Circuit has observed, “the FCC's considering national security under the public interest umbrella is not a new phenomenon,” but instead reflects “the kind of national security authority [the Commission] has exercised for decades.” *Huawei*, 2 F.4th at 439, 443. When Congress adopted the Secure Networks Act and the Secure Equipment Act, it did so against this established backdrop, demonstrating Congress's approval and ratification of it. *Cf. Haig*, 453 U.S. at 306 (holding that agency's

asserted power to revoke passports on national-security grounds was “‘sufficiently substantial and consistent’ to compel the conclusion that Congress has approved it”).

5. Hikvision’s contrary arguments rest on a myopic examination of individual terms and statutory provisions in isolation, divorced from the collective effect they contribute to Title III as a whole. But “[s]tatutory construction is a holistic endeavor,” and “statutory language must be read in its proper context and not viewed in isolation.” *Koons Buick Pontiac GMC, Inc. v. Nigh*, 543 U.S. 50, 60 (2004). “In expounding a statute, we must not be guided by a single sentence or member of a sentence, but look to the provisions of the whole law, and to its object and policy.” *Kelly v. Robinson*, 479 U.S. 36, 43 (1986) (quoting *United States v. Heirs of Boisdoré*, 49 U.S. (8 How.) 113, 122 (1849)). And as the 2022 Order explains, these “collective sources of statutory authority” together belie any claim that the Commission is powerless “to determine not to authorize [certain] equipment in the event that a national security agency determines that the equipment poses an unacceptable risk to our national security.” 2022 Order ¶ 43 (JA____—).

Reading these provisions collectively also requires that they be read in light of the Secure Equipment Act. “Look[ing] to the entire body of

relevant law” includes the “principle * * * that subsequent laws can affect a statute’s meaning.” *Huawei*, 2 F.4th at 445. Here, “that body of law now includes a statute showing Congress’s approval of the FCC’s assertion of authority” to consider national security risks when making equipment authorization decisions. *Ibid.* And when Congress enacted the Secure Equipment Act, it had before it the *2021 NPRM*’s explication of the Commission’s preexisting Title III authority to take such actions, which Congress is best understood to have thereby ratified. *See 2022 Order* ¶ 42 (JA____) (“Congress clearly intended to ratify the Commission’s tentative conclusions in the *NPRM* that it had authority as discussed therein.”).

Hikvision’s claim that this reading of the Commission’s preexisting authority would render the Secure Equipment Act meaningless (Br. 31–33) is mistaken. Congress may sensibly pass legislation ratifying or reinforcing agency authority simply to remove any possible doubt in response to threatened litigation, without implying that that the agency action would otherwise have been unlawful. Indeed, the Secure Networks Act did just that. After the Commission acted to prohibit certain federal subsidies from being used to purchase equipment from entities that pose a national security threat, Congress enacted the Secure

Networks Act to codify a materially similar requirement. In *Huawei*, the Fifth Circuit held that the Commission's actions were authorized under its pre-Secure Networks Act authority and that Congress's subsequent codification of similar authority did not call that into doubt. *See* 2 F.4th at 444–45. So too here, Congress's belt-and-suspenders approach in adopting the Secure Equipment Act supplies further support for the Commission's authority, not reason to doubt it.

CONCLUSION

For the foregoing reasons, Hikvision's petition for review of the *2025 Order* should be dismissed or otherwise denied.

Dated: April 23, 2026

Respectfully submitted,

/s/ Scott M. Noveck

D. Adam Candeub
General Counsel

Jacob M. Lewis
Deputy General Counsel

Sarah E. Citrin
Deputy Associate General Counsel

Scott M. Noveck
Counsel

FEDERAL COMMUNICATIONS
COMMISSION

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

*Counsel for Respondent Federal
Communications Commission*

Brett A. Shumate
Assistant Attorney General

Eric D. McArthur
*Deputy Assistant
Attorney General*

Sharon Swingle
Simon G. Jerome
Attorneys

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

*Counsel for Respondent
United States of America[†]*

[†] 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 10,202 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/ Scott M. Noveck
Scott M. Noveck
Counsel for Respondents

STATUTORY ADDENDUM

STATUTORY ADDENDUM CONTENTS

	Page
Secure Equipment Act of 2021, Pub. L. No. 117-55, 135 Stat. 423.....	Add. 2
Communications Act of 1934, <i>as amended</i> , 47 U.S.C. §§ 151 <i>et seq.</i> :	
Sec. 1, 47 U.S.C. § 151	Add. 3
Sec. 4(i), 47 U.S.C. § 154(i)	Add. 4
Sec. 229, 47 U.S.C. § 229	Add. 4
Sec. 301, 47 U.S.C. § 301	Add. 5
Sec. 302, 47 U.S.C. § 302a	Add. 5
Sec. 303, 47 U.S.C. § 303	Add. 6
Communications Assistance for Law Enforcement Act (CALEA), Pub. L. No. 103-414, 108 Stat. 4279 (1994):	
Sec. 105, 47 U.S.C. § 1004	Add. 6
47 C.F.R. § 2.901	Add. 7
47 C.F.R. § 2.939	Add. 7

The Secure Equipment Act of 2021, Pub. L. No. 117-55, 135 Stat. 423 (codified as Note to 47 U.S.C. § 1601), provides:

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.

Section 1 of the Communications Act, 47 U.S.C. § 151, provides:

Sec. 1 [47 U.S.C. § 151]. Purposes of Act; creation of Federal Communications Commission.^[*]

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 communication, 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 hereby 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 Act].

* Where headings in the U.S. Code differ from headings in the session laws enacted by Congress, this addendum uses the congressionally enacted headings. Where the text varies, the congressionally enacted text appears in brackets.

Section 4(*i*) of the Communications Act, 47 U.S.C. § 154(*i*), provides:

Sec. 4 [47 U.S.C. § 154]. Provisions relating to the Commission.

* * *

(*i*) The Commission may perform any and all acts, make such rules and regulations, and issue such orders, not inconsistent with [this Act], as may be necessary in the execution of its functions.

* * *

Section 229 of the Communications Act, 47 U.S.C. § 229, provides in pertinent part:

Sec. 229 [47 U.S.C. § 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).

* * *

Section 301 of the Communications Act, 47 U.S.C. § 301, provides in pertinent part:

Sec. 301 [47 U.S.C. § 301]. License for radio communication or transmission of energy.

It is the purpose of [this Act], among other things, to maintain the control of the United States over all the channels of radio transmission; and to provide for the use of such channels, but not the ownership thereof, by persons for limited periods of time, under licenses granted by Federal authority, and no such license shall be construed to create any right, beyond the terms, conditions, and periods of the license. * * *

Section 302 of the Communications Act, 47 U.S.C. § 302a, provides in pertinent part:

Sec. 302 [47 U.S.C. § 302a]. Devices which interfere with radio reception.

(a) 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) 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.

* * *

Section 303 of the Communications Act, 47 U.S.C. § 303, provides in pertinent part:

Sec. 303 [47 U.S.C. § 303]. General powers of Commission.

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

* * *

(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;

* * *

(g) Study new uses for radio, provide for experimental uses of frequencies, and generally encourage the larger and more effective use of radio in the public interest;

* * *

(r) Make such rules and regulations and prescribe such restrictions and conditions, not inconsistent with law, as may be necessary to carry out the provisions of [this Act] * * *.

* * *

Section 105 of the Communications Assistance for Law Enforcement Act (CALEA), 47 U.S.C. § 1004, provides:

Sec. 105 [47 U.S.C. § 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 C.F.R. § 2.901 provides in pertinent part:

§ 2.901 Basis and purpose.

(a) In order to carry out its responsibilities under the Communications Act * * * and in order to promote efficient use of the radio spectrum, the Commission has developed technical standards and other requirements for radio frequency equipment and parts or components thereof. * * * [These rules] may require that such equipment be authorized under Supplier's Declaration of Conformity or receive a grant of certification from a Telecommunication Certification Body.

* * *

47 C.F.R. § 2.939 provides in pertinent part:

§ 2.939 Revocation, withdrawal, or limitation of equipment authorization.

(a) The Commission may revoke, or place limitations pursuant to paragraph (e) of this section on, any equipment authorization:

(1) For false statements or representations made either in the application or in materials or response submitted in connection therewith or in records required to be kept by § 2.938.

(2) If upon subsequent inspection or operation it is determined that the equipment does not conform to the pertinent technical requirements or to the representations made in the original application.

(3) If it is determined that changes have been made in the equipment other than those authorized by the rules or otherwise expressly authorized by the Commission.

(4) Because of conditions coming to the attention of the Commission which would warrant it in refusing to grant an original application.

(b) Revocation of an equipment authorization shall be made in the same manner as revocation of radio station licenses, except as provided in paragraph (d) of this section.

* * *

(e) The Office of Engineering and Technology (OET) and the Public Safety and Homeland Security Bureau (PSHSB) may place limitations on an existing authorization for covered equipment authorizations to prohibit continued importation or marketing, pursuant to the following procedures:

(1) OET and PSHSB will issue a public notice announcing the intent to limit the scope of equipment authorizations to prohibit the further importation or marketing of specified devices identified by class, type, or other description sufficient to identify the devices.

(2) The public notice will include an assessment of the impact of the proposed prohibition with consideration of public interest factors, including: the unacceptable risks the equipment was found to pose, the economic and supply chain impacts, and any other criteria as specified by the Commission. The public notice should give particular weight to the specific determination(s), and any accompanying rules or analyses, through which the relevant equipment was added to the Covered List.

(3) The public notice will provide for a public comment period of no less than 30 days.

(4) OET and PSHSB will review the submissions, may request additional information as may be appropriate, and must make their determination as to whether to place limitations on the existing authorization to prohibit the further importation or marketing of the relevant devices, providing the reasons for such decision.