United States Court of Appeals

FOR THE DISTRICT OF COLUMBIA CIRCUIT

Argued December 14, 2023 Decided April 2, 2024

No. 23-1032

HIKVISION USA, INC.,
PETITIONER

v.

FEDERAL COMMUNICATIONS COMMISSION AND UNITED STATES OF AMERICA,
RESPONDENTS

MOTOROLA SOLUTIONS, INC.,
INTERVENOR

Consolidated with 23-1073

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

Christopher J. Wright and *Russell M. Blau* argued the causes for petitioners. With them on the joint briefs were *Andrew D. Lipman*, *Timothy J. Simeone*, *John T. Nakahata*, *John R. Grimm*, *Deepika H. Ravi*, *Annick Banoun*, *James M. Cole*, and *Tobias S. Loss-Eaton*.

Matthew J. Dunne, Counsel, Federal Communications Commission, argued the cause for respondents. With him on the brief were *Brian M. Boynton*, Principal Deputy Assistant Attorney General, U.S. Department of Justice, *Sharon Swingle* and *Casen Ross*, Attorneys, *Jacob M. Lewis*, Deputy General Counsel, Federal Communications Commission, and *Sarah E. Citrin*, Deputy Associate General Counsel.

Thomas M. Johnson Jr. argued the cause for intervenor in support of respondents. With him on the brief were *Bennett L. Ross* and *Michael J. Showalter*.

Before: MILLETT and PAN, *Circuit Judges*, and RANDOLPH, *Senior Circuit Judge*.

Opinion for the Court filed by *Circuit Judge* PAN.

PAN, *Circuit Judge*: Hikvision USA, Inc. ("Hikvision") and Dahua Technology USA Inc. ("Dahua") (collectively, "Petitioners") are two Chinese-owned companies that manufacture video cameras and video-surveillance equipment. In March 2021, the Federal Communications Commission ("FCC") relied on a congressional finding to place Petitioners' products on the "Covered List" — a list of communications equipment that poses a threat to U.S. national security. Later that year, in November 2021, Congress passed the Secure Equipment Act ("SEA"), which directed the FCC to no longer approve any equipment on the Covered List for marketing or sale within the United States. The FCC issued an order to implement the equipment ban mandated by the SEA. The ban applies to Petitioners' video-surveillance equipment to the extent that it is used for certain purposes, including "physical security surveillance of critical infrastructure."

Petitioners challenge the FCC's implementing Order, arguing that Petitioners' products do not belong on the Covered List and therefore should not be barred from U.S. markets. We hold that the SEA ratified the composition of the Covered List and leaves no room for Petitioners to challenge the placement of their products on that list under a predecessor statute. But we agree with Petitioners that the FCC's definition of "critical infrastructure" is overly broad. We therefore deny the petitions in part and grant them in part.

I.

Petitioners Hikvision and Dahua are U.S. subsidiaries of Chinese manufacturers of video equipment. In the United States, Petitioners' cameras are used by small- and medium-sized business owners to secure their premises. Industry commenters have expressed concern in FCC rulemakings that Petitioners' equipment could be utilized by the Chinese government to spy on sensitive American infrastructure and could pose other national-security risks. As a result, Petitioners' products have been specifically identified and addressed by both Congress and the FCC.

A.

In the John S. McCain National Defense Authorization Act for Fiscal Year 2019 ("NDAA"), Congress prohibited federal agencies from using or procuring certain "covered" technology sold by Chinese companies. Pub. L. No. 115-232, § 889, 132 Stat. 1636, 1917–19 (2018). The NDAA specifically targeted Petitioners' products for this limited ban from federal procurement. Section 889(f)(3) of the NDAA defines "covered telecommunications equipment" to include "video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company" that

is used "[f]or the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes." *Id.* at § 889(f)(3). Although the statute specifically names Petitioners' parent companies, the NDAA also applies to "any subsidiary or affiliate of such entities." *Id.*

Congress followed up in March 2020 by passing the Secure and Trusted Communications Networks Act ("SNA"). Pub. L. No. 116-124, 134 Stat. 158. The SNA instructed the FCC to create the Covered List, *i.e.*, to "publish on its website a list of covered communications equipment or services." 47 U.S.C. § 1601(a). The SNA also banned the use of FCC subsidies to purchase any equipment on the Covered List. *Id.* § 1602(a)(1). Equipment is designated as "covered" and "shall [be] place[d] on the list" if it "poses an unacceptable risk to the national security of the United States or the security and safety of United States persons." *Id.* § 1601(b)(1).[1] Section 1601(c) of the SNA requires the FCC to rely on four types of national-security determinations to place products on the Covered List. One of those determinations is the definition of "covered telecommunications equipment" under the NDAA. *Id.* § 1601(c)(3) (The Commission "shall place on the list" any equipment that "poses an unacceptable risk to national security . . . based solely on" such equipment "being covered telecommunications equipment or services, as defined in

[1] The equipment also must be "capable of" certain functions, including "routing or redirecting user data traffic or permitting visibility into any user data or packets," "causing the network of a provider of advanced communications service to be disrupted remotely," or "otherwise posing an unacceptable risk to the national security of the United States or the security and safety of United States persons." 47 U.S.C. § 1601(b)(2).

section 889(f)(3) of the [NDAA].").[2] The SNA requires the FCC to periodically update the Covered List, and specifically contemplates that communications equipment or services may be added or removed from the list. *Id*. § 1601(d); 47 C.F.R. §§ 1.50002, 1.50003 (implementing SNA).

In December 2020, the FCC began implementing the requirements of the SNA by issuing the Supply Chain Second Order. That Order established procedures and criteria for compiling the Covered List, including a "requirement to accept determinations" of national-security risk by certain sources. *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Second Report and Order (*Supply Chain Second Order*), 35 FCC Rcd. 14284, paras. 13, 58–71 (2020). One mandatory source was the section of the NDAA in which Congress determined that Petitioners' equipment posed national-security risks when used for listed purposes. *Supply Chain Second Order*, at paras. 66–71.

On March 12, 2021, the FCC officially published the Covered List, which included Petitioners' "[v]ideo surveillance and telecommunications equipment." *Public Safety and Homeland Security Bureau Announces Publication of the List of Equipment and Services Covered by Section 2 of the Secure*

---

[2] The other qualifying determinations include: (i) "A specific determination made by any executive branch interagency body with appropriate national security expertise, including the Federal Acquisition Security Council established under section 1322(a) of title 41"; (ii) "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)"; and (iii) "A specific determination made by an appropriate national security agency." 47 U.S.C. §§ 1601(c)(1)–(2), (4).

Networks Act, WC Docket No. 18-89, Public Notice, DA 21-309 (PSHSB, Mar. 12, 2021). In keeping with the statutory text of the NDAA, the Covered List included Petitioners' technology only "to the extent it [was] used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes." *Id*. As a result of Petitioners' inclusion on the Covered List, federal subsidies administered by the FCC could no longer be used to purchase Petitioners' products for listed purposes. *See* 47 U.S.C. § 1602(a)(1); *Supply Chain Second Order*, at para. 94.

B.

Under the Communications Act, the FCC is authorized to regulate devices that emit radiofrequency energy that could interfere with radio communications. 47 U.S.C. § 302a(a). In carrying out its regulatory responsibilities, the FCC has utilized an equipment-authorization program to ensure that radiofrequency-emitting devices comply with the FCC's requirements before they can be marketed in or imported into the United States. *See* 47 C.F.R. Part 2 Subpart I, § 2.801 *et seq*. (Marketing of Radio Frequency Devices); 47 C.F.R. Part 2 Subpart J, § 2.901 *et seq*. (Equipment Authorization Procedures); 47 C.F.R. Part 2 Subpart K, § 2.1201 *et seq*. (Importation of Devices Capable of Causing Harmful Interference).

In June 2021, the FCC issued a Notice of Proposed Rulemaking ("NPRM") that proposed banning the authorization of equipment on the Covered List. In the NPRM, the Commission sought comments on "various steps that [it] could take in its equipment authorization program . . . to reduce threats posed to our nation's communications system." J.A. 37. The FCC contemplated revising the equipment-authorization

rules to "prohibit authorization of any 'covered' equipment on the Covered List." *Id*. Petitioners were named on the first page of the NPRM's "Discussion" section as companies to whom the proposed ban would apply in some degree. After the NPRM's issuance, the FCC received a host of comments, some of which expressed uncertainty about whether the Secure Networks Act, the Communications Act, or any other statute empowered the FCC to ban equipment authorizations due to national-security concerns. Petitioners filed comments arguing that the FCC lacked statutory authority to promulgate the proposed rule.

Five months later, in November 2021, Congress passed the Secure Equipment Act. Pub. L. No. 117-55, 135 Stat. 423. The SEA directed the Commission to "adopt rules in the proceeding initiated" in the NPRM and specifically identified the NPRM by docket number. *Id*. at § 2(a)(1). In section 2(a)(2) of the SEA, Congress required the Commission to "no longer review or approve any application for equipment authorization for equipment that is on the [Covered List]," *i.e.*, "the list of covered communications equipment or services published by the Commission under" the Secure Networks Act. *Id*. at § 2(a)(2). Congress referred to the Covered List without commenting on its composition or altering its existing scope. *Id*.

A year later, in November 2022, the FCC issued the Order that Petitioners now challenge. As mandated by Congress in the SEA, the Order promulgates the rule contemplated by the NPRM: It bans equipment authorizations for "covered" equipment. The Order's ban applies to products on the Covered List, including video surveillance and telecommunications equipment manufactured by Petitioners Hikvision and Dahua, to the extent that such equipment is used for "the purpose of public safety, security of government

facilities, physical security surveillance of critical infrastructure, or other national security purposes." J.A. 186. Petitioners' products will not be authorized for sale in the United States "until such time as the Commission approves these entities' plans and measures . . . to ensure [that] such equipment will not be marketed and sold" for prohibited purposes. *Id.*

The Order also provides further guidance about when equipment is used for "physical security surveillance of critical infrastructure." In defining "critical infrastructure," the FCC cited several sources. First, the Commission "appl[ied] the meaning" provided by section 1016(e) of the USA PATRIOT Act of 2001 ("the Patriot Act"), which defines "critical infrastructure" as "'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.'" J.A. 210 (quoting 42 U.S.C. § 5195c(e)). Next, the Commission noted that Presidential Policy Directive 21 ("PPD-21") identifies sixteen critical infrastructure economic sectors;[3] and that the Cybersecurity and Infrastructure Security Agency ("CISA"), through the National Risk Management Center ("NRMC"), has published a set of fifty-five National Critical Functions to "guide national risk management

[3] The sixteen critical infrastructure sectors identified in PPD-21 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." J.A. 210–11.

efforts."[4] J.A. 210–11 & nn. 527 & 529 (citing Directive on Critical Infrastructure Security and Resilience, 1 Pub. Papers 106, 115 (Feb. 12, 2013); National Risk Management Center, Cybersecurity and Infrastructure Security Agency, *National Critical Functions Status Update to the Critical Infrastructure Community* 2–8 (2020)).

After observing that the CISA/NRMC guide adopts a definition of National Critical Functions that is similar to the Patriot Act's definition of critical infrastructure, the FCC found that, for the purposes of implementing the Order, "any systems or assets, physical or virtual, *connected to* the sixteen critical infrastructure sectors identified in PPD-21 or the 55 [National Critical Functions] identified in [the] CISA/NRMC [risk management guide] could reasonably be considered 'critical infrastructure.'" J.A. 211 (emphasis added). The Order then notes that the agency will continue to "develop further clarifications to inform applicants for equipment authorizations" and provide "more specificity and detail." *Id*.

---

[4] The CISA is a component of the Department of Homeland Security that seeks to defend against risks to physical and digital infrastructure. *About CISA*, CISA, https://perma.cc/KXP5-D5FZ (last visited Mar. 13, 2024). The NRMC is a center within CISA that focuses on strategic risk reduction, including initiatives to reduce risks in 5G technology, election security, pipeline cybersecurity, and more. *National Risk Management Center Fact Sheet*, CISA, https://perma.cc/YP53-E96G (last visited Mar. 13, 2024). The CISA/NRMC National Critical Functions Set includes activities such as "provid[ing] cable access network services," "distribut[ing] electricity," "conduct[ing] elections," "provid[ing] metals and materials," and "supply[ing] water." National Risk Management Center, Cybersecurity and Infrastructure Security Agency, *National Critical Functions Status Update to the Critical Infrastructure Community* 2–8 (2020) (capitalization altered throughout).

Petitioners timely filed their petitions for review of the November 2022 Order. We have jurisdiction under 28 U.S.C. § 2342(1) and 47 U.S.C. § 402(a).

II.

Under the Administrative Procedure Act, a court must set aside agency action that is arbitrary, capricious, an abuse of discretion, or otherwise contrary to law. 5 U.S.C. § 706(2)(A). "In the absence of statutory authorization for its act, an agency's action is plainly contrary to law and cannot stand." *Atlantic City Elec. Co. v. FERC*, 295 F.3d 1, 8 (D.C. Cir. 2002) (cleaned up); *see also Ball, Ball & Brosamer, Inc. v. Reich*, 24 F.3d 1447, 1450 (D.C. Cir. 1994) ("An agency can neither adopt regulations contrary to statute, nor exercise powers not delegated to it by Congress."). For an arbitrary-and-capriciousness challenge, "[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.) Corp. v. FCC*, 57 F.4th 256, 265 (D.C. Cir. 2022) (alteration in original) (quoting *FCC v. Prometheus Radio Project*, 141 S. Ct. 1150, 1158 (2021)).

III.

The FCC Order at issue bans the authorization of Petitioners' products for marketing and sale in the United States, to the extent that the products are used "for the purpose of . . . physical security surveillance of critical infrastructure." J.A. 209. Petitioners challenge two aspects of the Order. First, Petitioners argue that the FCC exceeded the scope of its statutory authority when it placed Petitioners' equipment on the Covered List. Second, Petitioners argue that the FCC's definition of "critical infrastructure" is overbroad and inconsistent with the NDAA. We reject Petitioners' claim that

their equipment does not belong on the Covered List, but we agree that the Commission's definition of critical infrastructure is too broad.

A.

The FCC's Order implemented the Secure Equipment Act of 2021, in which Congress directed the FCC to no longer "review or approve any application for equipment authorization for equipment that is on [the Covered List]." Pub. L. No. 117-55, § 2(a)(2), 135 Stat. 423, 423. Petitioners' video-surveillance and telecommunications equipment is on the Covered List — and was on it at the time Congress passed the SEA — and therefore is subject to the authorization ban. But Petitioners attempt to dispute the FCC's prior decision to place their products on the Covered List, arguing that the FCC misconstrued the SNA at that earlier point in time. According to Petitioners, they may make this belated claim because, during the 2022 rulemaking that led to the promulgation of the Order, the FCC "[r]eopened" the definition of covered equipment under the SNA. Reply Br. 5 (citing *Alvin Lou Media, Inc. v. FCC*, 571 F.3d 1, 8 (D.C. Cir. 2009)). The government contends that we lack jurisdiction to review Petitioners' untimely claim, which should have been made within 60 days of the disputed agency action (*i.e.*, the initial publication of the Covered List). Resp. Br. 38 (citing 28 U.S.C. § 2344).

In our view, Petitioners' argument does not implicate our jurisdiction. We have jurisdiction over this case because Petitioners timely filed petitions for review of the 2022 Order, contending that the Order's equipment-authorization ban was improperly applied to their products. *See* 28 U.S.C. § 2344. Our refusal to reach the merits of Petitioners' SNA argument is rooted not in jurisdictional concerns, but in our interpretation

of the SEA: The SEA ratified the composition of the Covered List at the time of the SEA's enactment and thus precludes Petitioners from claiming that their products were improperly put on the list at an earlier point in time.

Congress has clearly expressed its view that Petitioners' products pose a risk to national security in certain circumstances. It first did so in the NDAA, which prohibited executive agencies from procuring "video surveillance and telecommunications equipment produced by [Petitioners]" when used for certain purposes. Pub. L. No. 115-232, § 889(a), (f)(3), 132 Stat. 1636, 1917–18 (2018). Less than two years later, in the SNA, Congress directed the FCC to create a Covered List of equipment that "pose[s] an unacceptable risk to the national security of the United States," 47 U.S.C. § 1601(b)(2)(c), including communications equipment that is also "covered telecommunications equipment . . . as defined in section 889(f)(3) of the [NDAA]," *id.* § 1601(c)(3). The FCC then placed Petitioners' equipment on the Covered List and published the Covered List on its website. *Public Safety and Homeland Security Bureau Announces Publication of the List of Equipment and Services Covered by Section 2 of the Secure Networks Act*, WC Docket No. 18-89, Public Notice, DA 21-309 (PSHSB, Mar. 12, 2021).

Against that backdrop, Congress took aim at Petitioners again in the Secure Equipment Act. The SEA was enacted in response to controversy over the FCC's equipment-authorization NPRM. Congress passed the SEA to remove any doubt that the FCC was empowered to issue the equipment-authorization ban that Petitioners currently challenge. The SEA requires the FCC to promulgate the proposed rule that would ban authorizations for "equipment that is on the list of covered communications equipment . . . published by" the Commission. 135 Stat. at 423. As explained below, when

Congress directed the FCC to follow through on its NPRM and to prohibit the authorization of equipment that is on the Covered List, Congress was fully aware that (1) the NPRM specifically discussed Petitioners' products in connection with the proposed ban, and (2) Petitioners' products were on the Covered List. It appears, then, that when Congress passed the SEA, it intended to *require* the FCC to prohibit the marketing and sale of Petitioners' products for listed purposes within the United States.

Section 2(a) of the SEA reads as follows:

> (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)).

135 Stat. at 423.

Thus, subsection (1) identifies by docket number the NPRM in which the FCC proposed to ban authorizations of equipment on the Covered List: It orders the FCC to adopt rules pursuant to that specifically described NPRM. The NPRM referred to Petitioners, by name, as entities whose products would no longer be authorized for listed purposes. Meanwhile, subsection (2) mandates that the rules adopted in connection with the NPRM must carry out the FCC's proposed ban of authorizations of equipment "that is on the list of covered communications equipment or services published by the Commission." 135 Stat. at 423. Subsection (2) explicitly refers to the Covered List, which included Petitioners' products at the time of the SEA's passage.

The text and historical context of the SEA demonstrate that Congress incorporated the Covered List into the SEA, and thereby ratified the composition of the list. "[W]here . . . Congress adopts a new law incorporating sections of a prior law, Congress normally can be presumed to have had knowledge of the interpretation given to the incorporated law . . . ." *Lorillard v. Pons*, 434 U.S. 575, 581 (1978). But we need not rely on a presumption here because when Congress incorporated the Covered List into the SEA, it plainly was aware that Petitioners' equipment was on the Covered List: Not only was the list publicly available, but Congress itself identified Petitioners' products as national-security risks in the NDAA and then, in the SNA, made that determination relevant to the FCC's decision whether to place certain communications equipment on the Covered List. *See Jackson v. Modly*, 949

F.3d 763, 773 (D.C. Cir. 2020) (noting that an indication of congressional acquiescence is "particularly strong if evidence exists of the Congress's awareness of and familiarity with such an interpretation"). Moreover, the text of the SEA refers to the NPRM, which was explicit that Petitioners' equipment would be subject to the proposed authorization ban. And the legislative history of the SEA includes a specific reference to Petitioners' parent companies. *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) ("The [SEA] 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."). In short, the evidence of Congress's awareness of the contents of the Covered List could not be clearer.

Thus, when Congress referred to the Covered List in the SEA without questioning or discussing the makeup of that list, Congress affirmatively ratified the Covered List as it existed at the time of the SEA's passage. *See Bragdon v. Abbott*, 524 U.S. 624, 631 (1998) ("Congress' repetition of a well-established term carries the implication that Congress intended the term to be construed in accordance with pre-existing regulatory interpretations."); *cf. Forest Grove Sch. Dist. v. T.A.*, 557 U.S. 230, 239–40 (2009) ("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." (quoting *Lorillard*, 434 U.S. at 580)); Antonin Scalia & Bryan A. Garner, *Reading Law: The Interpretation of Legal Texts* 322–26 (2012) (discussing the

"prior-construction canon").[5] And when Congress targeted the Covered List for the equipment-authorization ban, it demonstrated its specific intent to prohibit the sale and marketing of Petitioners' products in the United States for listed purposes.

The Supreme Court has found congressional ratification of agency actions and judicial interpretations in analogous situations. In *Lorillard v. Pons*, for example, the Supreme Court determined that when Congress enacted the Age Discrimination in Employment Act ("ADEA") of 1967, it was aware of the prevailing judicial interpretations of the incorporated provisions of the Fair Labor Standards Act ("FLSA"). 434 U.S. at 580–82. Because "courts had uniformly afforded jury trials" under the enforcement provisions of the FLSA, the Court concluded that Congress intended that trials by jury would also be available under the ADEA. *Id*. at 585. Similarly, in *Bragdon v. Abbott*, the Court held that the Americans with Disabilities Act's ("ADA") definition of "disability" included individuals with HIV

---

[5] The ratification doctrine is frequently discussed in the context of Congress's reenactment of statutes. *See Thompson v. Clifford*, 408 F.2d 154, 164 (D.C. Cir. 1968) ("[T]he canon of statutory construction that reenactment without change after a course of administrative interpretation is tantamount to legislative ratification of the interpretation" rests on the reasoning "either that those in charge of the amendment are familiar with existing rulings, or that they mean to incorporate them." (quotation marks omitted)); *United States v. Bd. of Comm'rs of Sheffield, Ala.*, 435 U.S. 110, 135 (1978) (concluding that when "there had been a longstanding administrative interpretation of a statute when Congress re-enacted it, and . . . the legislative history of the re-enactment showed that Congress agreed with that interpretation, . . . Congress had ratified it"). The same principles apply with even greater force here, where Congress so clearly intended to incorporate the existing Covered List.

because the statute's definition was drawn "almost verbatim" from the definition of "handicapped individual" in the Rehabilitation Act of 1973. 524 U.S. at 631. A 1988 Department of Justice Office of Legal Counsel ("OLC") opinion had concluded that the Rehabilitation Act protected HIV-infected individuals. *Id*. at 642. The Court observed that "[a]ll indications are that Congress was well aware of the position taken by OLC when enacting the ADA and intended to give that position its active endorsement." *Id*. at 645. Like in *Lorillard* and *Bragdon*, "all indications" here are that Congress was "well aware" of the legal and administrative landscape when it enacted the SEA; and we thus infer that Congress intended the equipment-authorization ban to apply to all products that were on the Covered List at that time. *But see Public Citizen, Inc. v. HHS*, 332 F.3d 654, 668–69 (D.C. Cir. 2003) (declining to find ratification where there was no evidence that Congress was aware of the relevant agency action).

Petitioners contend that the SEA addresses only the consequences of being on the Covered List, while the SNA addresses *who* should be on the List. They argue that, because their products do not meet the statutory definition of "communications equipment" in the SNA, they cannot properly be on the Covered List or be subject to the equipment-authorization ban. We disagree. Petitioners seek to challenge their placement on the Covered List, which occurred before Congress enacted the SEA. But when Congress specified in the SEA that equipment on the Covered List would no longer be eligible for authorizations, Congress required that the ban would apply to Petitioners' equipment. Petitioners' objection to their inclusion on the Covered List under the SNA is thus foreclosed by Congress's "affirmative ratification of the [FCC's] administrative interpretation[]" of the content of the list. *Bragdon*, 524 U.S. at 646.

In sum, the 2022 Order implemented the SEA, which ratified the inclusion of Petitioners' products on the Covered List. Because Congress intended the FCC to ban the authorization of any equipment that was on the Covered List at the time of the SEA's enactment, Petitioners' claim that the FCC erred when it first placed Petitioners' equipment on the Covered List at an earlier time is irrelevant. Congress has "power to ratify the acts which it might have authorized" and such "ratification, if made, [is] equivalent to an original authority." *United States v. Heinszen*, 206 U.S. 370, 384 (1907). Even if Petitioners were correct that the FCC misinterpreted the SNA when it first placed Petitioners' products on the Covered List, Congress's ratification of the Covered List has foreclosed that claim.[6]

Finally, to the extent that there is any ambiguity, the national-security judgments and concerns underlying the Executive Branch's decision in this case counsel deference. *See Dep't of Navy v. Egan*, 484 U.S. 518, 530 (1988) ("[C]ourts traditionally have been reluctant to intrude upon the authority of the Executive in military and national security affairs."). As we have previously written, "[w]e cannot second-guess the FCC's judgment that allowing China to access this information poses a threat to national security." *Pac. Networks Corp. v. FCC*, 77 F.4th 1160, 1164 (D.C. Cir. 2023). That deference is redoubled by the repeated acts of Congress expressly identifying Petitioners' video-surveillance equipment as posing national-security risks. *See Fed. Express Corp. v. Dep't of Commerce*, 39 F.4th 756, 770 (D.C. Cir. 2022) (requiring the

---

[6] We hold only that Congress ratified the content of the Covered List when it enacted the SEA. We therefore need not reach the question of whether Congress ratified the interpretations of the SNA that the FCC employed when creating that list. We also do not express any view on Petitioners' arguments about the FCC's authority under the SNA.

"full force" of judicial deference on issues that "fall in the core of Executive and Legislative Branch expertise in the areas of national security and foreign affairs").

B.

Under the challenged Order, Petitioners' equipment is banned only when used "[f]or the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes." J.A. 209 (alteration in original). Petitioners take issue with the FCC's newly introduced definition of "critical infrastructure" in the Order. *See* Pet'rs' Br. 46 ("The Commission's interpretation of 'critical infrastructure' eviscerates the statutory limits and contravenes Congressional intent by treating nearly all aspects of the economy as 'critical infrastructure.'"). We agree with Petitioners that the Commission's interpretation is unjustifiably broad and is therefore arbitrary and capricious. *See* 5 U.S.C. § 706(2)(A).

The FCC relied on the Patriot Act, Presidential Policy Directive 21, and the Cybersecurity and Infrastructure Security Agency's set of National Critical Functions in crafting its definition of critical infrastructure. The Order states that "any systems or assets, physical or virtual, connected to the sixteen critical infrastructure sectors identified in PPD-21 or the 55 [National Critical Functions] identified in [the] CISA/NRMC [risk management guide] could reasonably be considered 'critical infrastructure.'" J.A. 211. Although Petitioners concede that the FCC's application of the Patriot Act definition of critical infrastructure may be appropriate, they assert that the Commission went too far in incorporating PPD-21 and the CISA National Critical Functions, as well as sweeping in anything that is merely "connected to" those economic sectors and functions. Pet'rs' Br. 54–57 (arguing that the FCC

"wrongly conflated multiple definitions of 'critical infrastructure' from different sources, without considering how they fit together or apply here").

The Commission's choice of reference materials — government sources that define "critical infrastructure" and related concepts in national-security contexts — was reasonable, and the Commission adequately explained why the cited sources were relevant. *See Motor Vehicle Mfrs. Ass'n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983) (noting that in determining whether an agency has provided a "satisfactory explanation," courts look for "whether the decision was based on a consideration of the relevant factors and whether there has been a clear error of judgment" (quotation marks omitted)). The Patriot Act defines "critical infrastructure" as "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. § 5195c(e). Meanwhile, PPD-21 identifies sixteen "critical infrastructure sectors," including commercial facilities, dams, emergency services, and food and agriculture. Directive on Critical Infrastructure Security and Resilience, 1 Pub. Papers 106, 114–15 (Feb. 12, 2013). And the CISA National Critical Functions Set includes activities such as "provid[ing] cable access network services," "distribut[ing] electricity," "conduct[ing] elections," "provid[ing] metals and materials," and "supply[ing] water." National Risk Management Center, Cybersecurity and Infrastructure Security Agency, *National Critical Functions Status Update to the Critical Infrastructure Community* 2–8 (2020) (capitalization altered throughout). The FCC's reliance on its chosen sources reflects appropriate consideration of relevant factors identifying "critical" areas of the economy that

have been vetted by those in the Executive Branch charged with assessing national-security risks. *See Republican Nat'l Comm. v. FEC*, 76 F.3d 400, 408 (D.C. Cir. 1996) ("[T]he Commission's new regulation results from exactly the kind of agency balancing of various policy considerations to which courts should generally defer."); *LaRose v. FCC*, 494 F.2d 1145, 1146 n.2 (D.C. Cir. 1974) (noting that part of the FCC's regulatory mandate is to "consider other federal policies").

But the definition of "critical infrastructure" ultimately adopted by the FCC includes any "systems or assets" that are merely "connected to" the sixteen sectors identified by PPD-21 or the fifty-five functions listed by the CISA risk-management guide. J.A. 211. The FCC failed to explain or justify its use of the expansive words "connected to," and the scope of the definition is therefore arbitrarily broad.

First, the Commission does not explain why everything "connected to" any sector or function that implicates national security must be considered "critical," especially in light of the Patriot Act's emphasis on particular "systems and assets" that are "vital to the United States." The FCC's definition threatens to envelop ever-broadening sectors of the economy. As Petitioners note, the FCC's definition reads the word "critical" out of the statute and applies the equipment-authorization ban to all "infrastructure." Pet'rs' Br. 56. It is entirely implausible that every single system or asset that is "connected to," for example, the food and agriculture sector, or to the function of supplying water, is "critical" to the national security of the United States. The FCC did not rebut Petitioners' argument that "coffee shops, residential apartment buildings, used car lots, and dry-cleaning stores" could all plausibly fall within the Commission's definition. *Id*. at 57. Indeed, at oral argument, the FCC was unable to identify any relevant infrastructure that would not be covered, whether critical or not. Oral Argument

at 52:28–53:50. Without further explanation of why its expansive interpretation is reasonable or consistent with the statute, the Commission's definition is not in accordance with law and is arbitrary and capricious. *See* 5 U.S.C. § 706(2)(A); *China Telecom*, 57 F.4th at 264 (agencies must "reasonably explain[]" their decisions (quotation marks omitted)).

Second, the FCC's definition fails to provide comprehensible guidance about what falls within the bounds of "critical infrastructure." Instead, the Order merely states that "any" systems or assets "connected to" a laundry list of economic sectors and functions "could reasonably be considered" critical infrastructure. J.A. 211. Although the FCC suggests that "[P]etitioners need only seek guidance from the Commission by submitting a request for a declaratory ruling," such a requirement is unworkable. Resp. Br. 57. The Commission has essentially frozen all sales of Petitioners' equipment in the United States until Petitioners can submit a marketing plan which demonstrates that their products will not be used for "physical security surveillance of critical infrastructure." J.A. 209. Without a clear understanding of what constitutes a "connect[ion] to" critical infrastructure, Petitioners will face significant difficulty in developing such a marketing plan. The FCC provides no justification for imposing such a burden on Petitioners. *See ACA Int'l v. FCC*, 885 F.3d 687, 700 (D.C. Cir. 2018) (Agency action is "arbitrary and capricious" if it "fails to articulate a comprehensible standard" and "offers no meaningful guidance to affected parties." (quotation marks omitted)).

Accordingly, we conclude that the FCC's definition of "critical infrastructure" as all systems and assets "connected to" sixteen economic sectors and fifty-five economic functions is overbroad, unexplained, and arbitrary.

* * *

For the foregoing reasons, we uphold the FCC's Order to the extent that it prohibits the authorization of Petitioners' equipment for sale and marketing in the United States for use in the physical security surveillance of critical infrastructure; but we vacate the portions of the FCC's order defining "critical infrastructure" and remand to the Commission to comport its definition and justification for it with the statutory text of the NDAA. *Ky. Mun. Energy Agency v. FERC*, 45 F.4th 162, 179–80 (D.C. Cir. 2022) ("Vacatur is the normal remedy for unsustainable agency action, and . . . the Commission . . . [has not] given us any reason to depart from that standard course of action." (cleaned up)).

So ordered.