HWG | HARRIS, WILTSHIRE & GRANNIS LLP

November 17, 2021

Ex Parte via ECFS

Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program, ET Docket No. 21-232

Dear Ms. Dortch:

Hikvision USA, Inc. ("Hikvision") files this letter to make clear that, notwithstanding the enactment of the Secure Equipment Act of 2021 ("SEA"),[1] the Commission has no statutory authority to exclude any Hikvision equipment—none of which is broadband network equipment—from the Commission's equipment authorization processes under Part 2 of the Commission's rules. The SEA did not expand the scope of the equipment that can be placed on the Covered List pursuant to the Secure and Trusted Communications Networks Act of 2019 ("SNA").[2] As its name suggests, the focus of the SNA was communications networks, not peripheral devices such as Hikvision's. Accordingly, the SNA only permits "communications equipment or service" to be placed on the Covered List,[3] and it specifically defines "communications equipment or service" to mean equipment "essential" to the provision of broadband.[4] None of Hikvision's equipment, specifically including its video surveillance cameras and network video recorders ("NVRs"), is essential to broadband service. And as Hikvision has already set forth in its comments, the Commission has no statutory authority under any other provision of the Communications Act of 1934, as amended (the "Communications Act"), to bar Hikvision equipment from authorization under the generally applicable provisions of Part 2 of its rules. Section 302 of the Communications Act only permits the equipment authorization regime to regulate radio frequency interference caused by devices. Section 303 does not provide any additional authority to exclude Hikvision devices from the Commission's equipment authorization processes, particularly for devices that are not radio stations. As such, the Commission has no authority to adopt the proposed rules with respect to Hikvision.

---

1 Secure Equipment Act of 2021, Pub. L. No. 117-55 § 2(a)(2) (2021) ("SEA").

2 Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 134 Stat. 158 (2020), as amended by Pub. L. No. 116-260, 134 Stat. 1182, 2120 (Dec. 27, 2020), and codified as 47 U.S.C. § 1601 *et seq*.

3 47 U.S.C. § 1601(b).

4 *Id.* § 1608(4).

Indeed, the Commission is statutorily compelled to remove Hikvision from the Covered List. Section 2(d)(2) of the SNA makes clear that the Commission must remove entities from the Covered List when the conditions on which their inclusion was based no longer exist. The fact that Hikvision equipment is not "communications equipment or service" fundamentally disqualifies Hikvision from inclusion on the Covered List for all products that are not essential to broadband. Hikvision hereby requests that the Commission immediately remove it from the Covered List.

Because the SEA did not expand the scope of equipment that can be listed on the Covered List, even if the Commission were somehow able to reach Hikvision's video surveillance equipment (which it cannot), the proposed rules could not apply to equipment, such as Hikmicro's thermal monoculars used by hunters and wildlife enthusiasts, that is neither telecommunications (of which there is none) or video surveillance equipment. With respect to video surveillance equipment, even if that equipment could fall within "communications equipment or service" (which it cannot), there is still no statutory authorization post-SEA to apply the new rules to uses of Hikvision video surveillance equipment other than for public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes.

In all events, the Commission cannot rely on the SEA as authority for the proposed rules because, if the SNA somehow *does* reach Hikvision's cameras, the SEA is an unconstitutional Bill of Attainder as applied to Hikvision. Because Hikvision was on the Covered List when the SEA was passed, the SEA applies to Hikvision with specificity. And the SEA would impose punishment by effectively excluding Hikvision from the U.S. market and branding it as disloyal and untrustworthy. The Bill of Attainder Clause prohibits such legislative punishments.

The Commission need not be concerned that applying the SNA and the SEA in accordance with the SNA's plain meaning would somehow create a gaping hole in the United States' national defense. The initial and reply comments overwhelmingly demonstrate that there is no basis for concluding that video surveillance equipment, like Hikvision's cameras and NVRs, poses any unique or material cybersecurity threat either to the nation's telecommunications infrastructure or to private businesses. As Hikvision has shown in its comments, replies, and supporting expert reports—including the attached expert report summary accompanying this filing[5]—its equipment can be, and frequently is, set up in configurations that are either not connected to the Internet and thus protect against cyberattacks, or that can be readily safeguarded through generally accepted cybersecurity best practices. Furthermore, the record shows that Hikvision equipment is no more—and often less—subject to cybersecurity vulnerabilities than its competitors' equipment. There is no factual basis for targeting Hikvision as a unique cybersecurity threat, and the Commission cannot adopt rules based on unsupported speculation. Accordingly, the Commission should not move forward to adopt rules that would

---

[5] Hikvision engaged FTI Consulting ("FTI") to conduct a cybersecurity assessment of a Hikvision camera and network video recorder. The Executive Summary section of FTI's assessment report was submitted to the Commission with this ex parte filing. *See generally* FTI Consulting, *Executive Summary, Hikvision Equipment Cybersecurity Assessment Report* (Nov. 2021) ("FTI Nov. 2021 Report").

bar Hikvision from utilizing the Supplier's Declaration of Conformity ("SDOC") and equipment authorization processes under Part 2.

I. THE PROPOSED RULES EXCEED THE COMMISSION'S LEGAL AUTHORITY.

A. Hikvision Products Fall Outside the Scope of the SEA and SNA.

The SEA does not expand the category of products for which the Commission may deny equipment authorizations. On the contrary, it simply requires the Commission to "clarify" that it will "no longer review or approve any application for equipment authorization for equipment *that is on the list of covered communications equipment or services*" that the Commission publishes pursuant to the SNA.[6] Accordingly, any authority granted by the SEA extends only to equipment properly within the scope of the SNA. Hikvision's video surveillance equipment does not fall within that scope. Moreover, many categories of products produced by Hikvision subsidiaries and affiliates have no relationship to telecommunications or video surveillance, and thus fall outside even an overbroad interpretation or application of the SNA.

1. Section 2(b)(1) of the SNA Does Not Permit Inclusion on the Covered List of Communications Equipment or Service that Is Not Essential to Broadband, and Thus Such Equipment Cannot Be Excluded from Equipment Authorization Pursuant to the SEA.

The SNA contains several express limitations on the scope of equipment and services that may be placed on the Covered List. The clearest and most significant of those limitations is that, to appear on the Covered List, such equipment or services must be "*communications* equipment or service."[7] The SNA specifically defines "communications equipment or service" as "any equipment or service that is essential to the provision of advanced communications service."[8] "Advanced communications service" is defined by the SNA to have the same meaning as the term "advanced telecommunications capability" in Section 706 of the Communications Act.[9] Thus, applying Section 706's definition, communications equipment under the SNA is limited to that which is "essential to the provision" of any "high-speed, switched, broadband telecommunications capability . . . ." [10] In other words, equipment is only "communications equipment" under the SNA if it is *essential to* the provision of *broadband service*.

There is no serious argument that the Hikvision video surveillance equipment that the Commission now purports to exclude from the Part 2 equipment authorization processes is

---

6 *See* SEA § 2(a)(2) (emphasis added).

7 47 U.S.C. § 1601(b) (emphasis added).

8 *Id.* § 1608(4).

9 *Id.* § 1608(1).

10 *Id.* § 1302(d)(1).

essential to the provision of such broadband service. The plain text of the SNA is unambiguous—the Commission can only place equipment on the Covered List if it meets the statutory definition of "communications equipment or service." *None* of Hikvision's video surveillance products sold in the United States are even "used in" broadband networks—the Commission's impermissibly overbroad interpretation of "essential" in the *Second Report and Order*[11]—let alone *essential* to the provision of broadband service.[12] Because Hikvision's products therefore do not meet the threshold definition of "communications equipment" as specifically and explicitly defined by the SNA, they cannot be placed—or retained—on the Covered List. And the Commission has no statutory authorization other than the SNA to place equipment on the Covered List.[13]

Moreover, as noted above, in its *Second Report and Order* implementing the SNA, the Commission interpreted "communications equipment and service" to "include all equipment or services *used in* fixed and mobile broadband networks, provided they include or use electronic components."[14] The Commission's broad interpretation is wholly inconsistent with any reasonable understanding of the term essential, for which the dictionary definition is "of the utmost importance: basic, indispensable, necessary."[15] Even this expansive definition of "essential," however, does not reach peripheral devices that are merely used on the end user's side, because being "used *in*"—the term the Commission adopted—is not the same as "used *with*" broadband networks.[16]

In its *Third Report and Order*, which implemented the SNA's "rip-and-replace" reimbursement program, the Commission further acknowledged that Internet of Things devices, which would include Hikvision security cameras and NVRs, are not used in broadband networks. In declining to reimburse replacement of these devices, the Commission stated,

---

[11] *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Second Report and Order, 35 FCC Rcd. 14284, ¶ 52 (2020) ("*Supply Chain Second Report and Order*" or "*Second Report and Order*") (emphasis added).

[12] As Hikvision noted in its comments, only about five percent of Hikvision devices sold in the United States contain radio transmitters, and thus only a small number are certified pursuant to the Commission's equipment certification process. *See* Hikvision Comments at 17.

[13] We note that, because Hikvision's equipment sold in the United States falls outside of the SNA's threshold definition of "communications equipment or service," all of Hikvision's jurisdictional arguments advanced in its opening and reply comments apply equally here.

[14] *Supply Chain Second Report and Order* ¶ 52.

[15] *Essential*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/essential (last visited Nov. 15, 2021).

[16] Although the Commission then stated "[w]e believe that all equipment or services that include or use electronic components can be reasonably considered essential to broadband networks," the Commission could not possibly have meant even if that equipment was not "used in" a broadband network. *Supply Chain Second Report and Order* ¶ 52. Otherwise, the SNA would extend to toasters and coffeemakers.

"Handsets and other customer premises equipment, including Internet of Things devices, used by end uses to access and utilize advanced communications services are distinctly different from the cell sites, backhaul, core network, etc. *used to operate a network and provide advanced communications services.*"[17] Of course, unlike mobile handsets, cable modems, and other network gateway CPE, Hikvision security cameras and NVRs are even further removed from broadband networks, as they operate behind such network access devices. Accordingly, the Commission itself has already found that Hikvision video surveillance devices are not "communications equipment and service" as defined in the SNA.

There is nothing in the legislative history of the SNA that indicates that Congress intended to reach equipment that was not essential to broadband networks. The title of the Secure and Trusted Communications Networks Act itself reflects a singular focus on communications network equipment, not peripheral devices that exist outside of, but may connect with, those networks. None of the House Report, the House floor debate, or the Senate floor debate contains any references to video surveillance equipment or to Hikvision.[18] Indeed, even the SNA's reference to Section 889 of the National Defense Authorization Act for Fiscal Year 2019 ("2019 NDAA") was limited to "communications equipment or service" that was "covered telecommunications equipment or services" under Section 889, *i.e.*, a subset of the Section 889 covered equipment.[19] The express objective of the SNA was to reach equipment in the broadband networks, and the language of the statute simply does not reach beyond those networks.

Nor does the fact that the Commission previously interpreted Section 2 of the SNA more broadly in creating the Covered List overcome this statutory obstacle, because the proposed rules directly implicate Hikvision in a way that the *Supply Chain Second Report and Order* and the Covered List did not. The purpose of the Covered List under the SNA, and its only substantive effect, was to bar equipment on the Covered List from being procured or maintained with universal service support.[20] Because Hikvision's equipment is not generally used in the provision of services supported by federal universal service support mechanisms, Hikvision was not harmed in a manner cognizable for standing purposes by the *Second Report and Order* or the issuance of the Covered List. Now, however, given the far broader sweep of the Commission's proposed regulations, the threshold question of what products can be placed on the Covered List has direct relevance to Hikvision. Moreover, the Commission is required by statute to "periodically update" the Covered List[21]—and therefore has a statutory obligation to remove entities from the Covered List if the conditions upon which they were included on the list do not

---

[17] *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Third Report and Order, FCC No. 21-86, WC Docket No. 18-89, ¶ 94 (rel. July 14, 2021) ("*Supply Chain Third Report and Order*").

[18] *See* H.R. Rep. No. 116-352 (2019); 165 Cong. Rec. H10,282–86 (daily ed. Dec. 16, 2019); 166 Cong. Rec. S1,236 (daily ed. Feb. 27, 2020).

[19] 47 U.S.C. § 1601(c)(3).

[20] *Id.* § 1602(a).

[21] *Id.* § 1601(d)(1).

apply. Given that Hikvision was incorrectly placed by the Commission on the Covered List in the first place, the Commission has an obligation to correct that error by updating the List to remove Hikvision.

The case law regarding the Hobbs Act is particularly instructive as to why consideration of these statutory arguments cannot be avoided by asserting that they are untimely requests to reconsider the *Second Report and Order*. The D.C. Circuit has made clear that judicial challenges to new *applications* of agency decisions are not barred by the sixty-day period for appeal generally prescribed by the Hobbs Act. At a minimum, the proposed rules go far beyond the *Second Report and Order*'s focus on USF subsidies. There is no reason Hikvision should have anticipated at the time of that order that the Commission would extend the application of the Covered List to other purposes—much less to effectively barring *all* sales of Hikvision video surveillance products, let alone products far outside the ambit of the SNA or the 2019 NDAA. In this situation, the Hobbs Act would not "foreclose subsequent examination of a rule where properly brought before this court for review of further Commission action applying it," and the Commission cannot avoid reexamining its earlier order.[22] In other words, the current proposal would "fundamentally alter[]" the preexisting regime and thus is subject to renewed challenge.[23]

2. Even If "Communications Equipment or Service" Could Include Video Surveillance Equipment, It Cannot Possibly Reach Equipment that Is Not Video Surveillance Equipment.

Even if the Commission were somehow to expand beyond the SNA's definition of "communications equipment or service," that definition is not the SNA's only limitation on the scope of equipment permitted to be included on the Covered List. Even if Hikvision equipment were "communications equipment," the statute also expressly states that Hikvision may be included on the Covered List "if and only if" it meets the separate and independent requirements of Sections 2(b)(1) and 2(b)(2) of the SNA.[24] Section 2(b)(1) provides that the equipment must have received one of the four determinations as to national security and safety set forth in

---

[22] *See Functional Music, Inc. v. FCC*, 274 F.2d 543, 546 (D.C. Cir. 1958); *Alvin Lou Media, Inc. v. FCC*, 571 F.3d 1, 8 (D.C. Cir. 2009) ("This court permits both constitutional and statutory challenges to an agency's application or reconsideration of a previously promulgated rule, even if the period for review of the initial rulemaking has expired.") (quotation marks and modifications omitted); *Nat'l Res. Def. Council v. EPA*, 513 F.3d 257, 260 (D.C. Cir. 2008) (noting "the established doctrine that parties claiming substantive invalidity of a rule for which direct statutory assault is time-barred are nonetheless free to raise their claims in actions against agency decisions *applying* the earlier rule") (emphasis in original).

[23] *MCI Telecomms. Corp. v. FCC*, 765 F.2d 1186, 1190–91 (D.C. Cir. 1985).

[24] 47 U.S.C. § 1601(b).

Section 2(c) of the SNA.[25] Yet the only such determinations made with respect *to Hikvision* are those set forth in Section 889(f)(3) of the 2019 NDAA.

Section 889(f)(3) of the 2019 NDAA applies to Hikvision (or its subsidiaries and affiliates) "[f]or the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes" only insofar as Hikvision produces "video surveillance and telecommunications equipment."[26] That is, Section 889(f)(3) applies only to Hikvision products that are (1) video surveillance equipment or telecommunications equipment, *and* (2) used for purposes of public safety, government or critical infrastructure security, or national security. Section 889 of the 2019 NDAA does not define "telecommunications equipment," but that term is defined by the Communications Act as "equipment, other than customer premises equipment, used by a carrier to provide telecommunications services, and includes software integral to such equipment (including upgrades)."[27]

As to Section 889(f)(3)'s first criterion, Hikvision and its subsidiaries produce numerous products that are *not* "video surveillance [or] telecommunications equipment" and therefore are not within the ambit of Section 889(f)(3). As just one example, Hikvision's subsidiary Hikmicro produces thermal monoculars "designed to give outdoor enthusiasts a portable way to see more in nature," binoculars, and scopes.[28] Such devices are not "telecommunications equipment" as that term is defined by the Communications Act, or under any possible definition of that term. Clearly, Hikmicro products intended for outdoor and hunting enthusiasts are not "used by a carrier to provide telecommunications services." Similarly, Hikmicro handheld temperature screening products[29] fall far afield of the definition of telecommunications equipment. Hikmicro's outdoor-use products are also plainly not "video surveillance" equipment within any reasonable definition: their purpose is to provide outdoor and hunting enthusiasts with enhanced visibility. These are but one example of Hikvision equipment that is neither video surveillance nor telecommunications equipment, and thus falls outside of any reading of the SNA.

3. Even as to Video Surveillance Equipment, the Proposed Rules Exceed the Purpose-Based Limitations in Section 2(b) of the SNA.

As noted above, the SEA does not expand the scope of equipment targeted by the SNA. In the SNA, Congress specified that equipment could be placed on the Covered List only to the extent that it meets the public safety-or-security use requirement under SNA Section 2(b)(1) *and*

---

[25] *Id.* § 1601(b)(1).

[26] National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 889(f)(3)(B), 132 Stat. 1636, 1918 (2018) ("2019 NDAA").

[27] 47 U.S.C. § 153(52).

[28] *See, e.g.*, *Monocular*, HIKMICRO, https://www.hikmicrotech.com/en/product-c/4 (last visited Nov. 15, 2021).

[29] *See, e.g, Handheld,* HIKMICRO, https://www.hikmicrotech.com/en/product-b/14 (last visited Nov. 15, 2021).

also is capable of the functions outlined in SNA Section 2(b)(2). Neither condition is satisfied with respect to Hikvision's video surveillance equipment.

a. As to Video Surveillance Equipment, the Proposed Rules Exceed the Limitations in Section 2(b)(1) of the SNA.

To meet the first criterion in Section 2(b)(1) using Section 889 of the 2019 NDAA for inclusion in the Covered List, Hikvision equipment must be used for statutorily-specified purposes. Specifically, Section 889 defines "covered telecommunications or service" as "video surveillance and telecommunications equipment produced by" Hikvision "[f]or the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes."[30] In the *Supply Chain Second Report and Order*, the Commission recognized as much, stating that "we will incorporate onto the Covered List such equipment from . . . Hikvision" only "to the extent it is used for public safety or security."[31] The Covered List itself repeats this limitation.[32] Although neither the SNA nor the Commission has specifically defined terms like "public safety" or "surveillance of critical infrastructure," Congress plainly intended the narrowness of this language to impose meaningful limitations on the circumstances in which equipment could be placed on the Covered List. Congress could have included equipment used for "safety," for example, or for surveillance of "infrastructure"—but *public* safety and *critical* infrastructure are necessarily narrower terms.

Of course, as set forth in Hikvision's opening comments, its video surveillance equipment is typically used for *private security*, to secure small and medium-sized businesses.[33] Such uses have nothing to do with *public* safety, *critical* infrastructure, *government* facilities, or *national* security. To find otherwise would render those qualifying terms meaningless. Such uses outside of the public safety and security context fall outside of Section 889 and therefore are not appropriate for inclusion on the Covered List.

Motorola acknowledges that "the Covered List is predicated on 'covered telecommunications equipment or services, as defined in section 889(f)(3)' of the 2019

---

30 2019 NDAA § 889(f)(3)(B).

31 *Supply Chain Second Report and Order* ¶ 68.

32 *Public Safety and Homeland Security Bureau Announces Publication of the List of Equipment and Services Covered by Section 2 of the Secure Networks Act*, Public Notice, DA No. 21-309, WC Docket No. 18-89, App'x (rel. Mar. 12, 2021) (listing Hikvision equipment only "to the extent it is used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, including telecommunications or video surveillance services produced or provided by such entity or using such equipment").

33 *See generally* Comments of Hikvision USA, Inc. (Corrected) at 2, 36, ET Docket No. 21-232 (filed Sept. 20, 2021) ("Hikvision Comments").

NDAA,"[34] but it then appears to essentially urge the Commission to ignore the plain language of the SNA. Rather than referencing that narrow, specific language in the SNA, Motorola claims that vague "security risks" justify placing equipment on the Covered List.[35] That is simply inconsistent with the statute. Motorola's argument also ignores the General Services Administration's guidance to government contractors that Section 889's prohibitions apply to Hikvision *only if* Hikvision's equipment is used "[f]or the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes."[36] If Hikvision's equipment is not used for these purposes, then it is not covered by Section 889[37] and cannot be included on the Covered List, and thus falls outside the scope of the SEA. It also falls outside the scope of the SEA because it falls outside of the Covered List's specific listing itself.

b. As to Video Surveillance Equipment, the Proposed Rules Lack the Capabilities Required by Section 2(b)(2) of the SNA.

Independently, the plain language of the SNA also permits Hikvision's equipment to be placed on the Covered List only if it also meets the functionality requirements under Section 2(b)(2) of the SNA, *i.e.*, is "capable of (A) routing or redirecting user data traffic or permitting visibility into any user data or packets that such equipment or service transmits or otherwise handles; (B) causing the network of a provider of advanced communications service to be disrupted remotely; or (C) otherwise posing an unacceptable risk to the national security of the United States or the security and safety of United States persons."[38]

As already explained in Hikvision's opening and reply comments, Hikvision cameras and NVRs are incapable of routing or redirecting user data traffic, permitting visibility into user data,[39] or causing disruption of an advanced communications network. They merely generate video signals, and do not "route" those signals.[40] And, when Hikvision devices are deployed in

---

[34] Reply Comments of Motorola Solutions, Inc. at 11, ET Docket No. 21-232 (filed Oct. 18, 2021) ("Motorola Reply").

[35] *Id.* at 11–12.

[36] Hikvision Comments at 36–37, 36 n.80 (quoting 2019 NDAA § 889(f)(3)(B)); *see also* U.S. Gen. Servs. Admin. SCRM Rev. Bd., *SCRM Criteria for Section 889 Part B*, at 1 (Aug. 13, 2020), https://www.gsa.gov/cdnstatic/SCRM%20review%20board%20889%20PART%20B%20Rubric_0.pdf.

[37] *See* Hikvision Comments at 36–37.

[38] 47 U.S.C. § 1601(b)(2).

[39] Hikvision Comments at 37–39; Reply Comments of Hikvision USA, Inc. at 6–7, ET Docket No. 21-232 (filed Oct. 18, 2021) ("Hikvision Reply").

[40] Hikvision Comments at 38; Hikvision Reply at 6.

a standalone video surveillance installation, they are not capable of routing or redirecting user data traffic or permitting visibility into user data.[41]

Hikvision cameras and NVRs do not pose a national safety risk, nor do they threaten Americans' safety or security—to the contrary, Hikvision products are used to *enhance* private businesses' safety and security. Hikvision products therefore fail to meet another threshold requirement for inclusion on the Covered List: the functionality requirements under Section 2(b)(2).

II. THE SEA IS UNCONSTITUTIONAL AND CANNOT SUPPLY THE COMMISSION WITH AUTHORITY TO ENACT ITS PROPOSED RULES.

Hikvision's comments and reply comments demonstrated that the Commission's proposal to deny equipment authorizations to Chinese companies simply because they are on a list of Chinese companies is unconstitutional. The fact that Congress has now instructed the Commission to do what the Commission already intended to do does not alter the constitutional defects in the Commission's proposed rule, because Congress, too, is constrained by the Constitution. Indeed, at the most fundamental level, because the Commission cannot exercise any authority Congress has not delegated to it, and because Congress plainly cannot delegate authority it does not have, nothing in the SEA overcomes the constitutional infirmities we first identified in our comments.

A. The SEA is an Unconstitutional Bill of Attainder.

If—contrary to the plain statutory language discussed above—the SNA reaches Hikvision's equipment and the SEA bars authorization regardless of the purpose the equipment is used for, then the SEA is an unconstitutional bill of attainder and cannot support the Commission's proposed rules. Article I of the Constitution mandates that "No Bill of Attainder . . . shall be passed."[42] A bill of attainder is legislation that targets and punishes a specific person or entity—"a law that legislatively determines guilt and inflicts punishment upon an identifiable individual without provision of the protections of a judicial trial."[43] A law violates the Bill of Attainder Clause if "it (1) applies with specificity and (2) imposes punishment."[44] Both are true here: Congress has specifically targeted Hikvision, and it has punished the company by purporting to instruct the Commission to exclude it from the United States and by branding it as disloyal.

Because all radio frequency devices must receive Commission equipment authorization to be marketed in the United States, the SEA would punish Hikvision by prohibiting the importation, marketing, sale, or use of the Hikvision products on the Covered List. If the SNA reaches all Hikvision video surveillance equipment, and if the SEA applies however that

---

41 Hikvision Comments at 38; Hikvision Reply at 7.

42 U.S. Const. art. I, § 9, cl. 3.

43 *Nixon v. Adm'r of Gen. Servs.*, 433 U.S. 425, 468 (1977).

44 *Foretich v. United States*, 351 F.3d 1198, 1217 (D.C. Cir. 2003) (citation omitted).

equipment is used, then this prohibition applies to most of Hikvision's products in this market, accounting for the vast majority of its U.S. sales. The SEA thus would effectively ban Hikvision from the United States without ever letting the company address the concerns supposedly motivating the listing, escape the listing by satisfying neutral standards, or seek judicial review of its listing or continued listing.

1. The SEA Applies to Hikvision With Specificity.

The first element is easily met here. "The element of specificity may be satisfied if the statute singles out a person or class by name or applies to 'easily ascertainable members of a group.'"[45] The SEA applies to "equipment that is on the list of covered communications equipment or services published by the Commission under" the SNA.[46] When Congress passed the SEA, Hikvision was on the Covered List—indeed, it was one of just five listed companies. The SEA thus applies to Hikvision with specificity and will continue to do so unless the FCC removes Hikvision from the Covered List.

2. The SEA Is Punitive.

The SEA is also punitive. "Punishment" under the Bill of Attainder Clause is not limited to criminal sanctions. Rather, "the deprivation of any rights, civil or political, previously enjoyed, may be punishment."[47] To determine whether a deprivation rises to that level, courts consider three factors: "(1) Whether the challenged statute falls within the historical meaning of legislative punishment; (2) whether the statute, viewed in terms of type and severity of burdens imposed, reasonably can be said to further nonpunitive legislative purposes; and (3) whether the legislative record evinces a congressional intent to punish."[48] The second factor—the "functional test" of punishment—is the "most important."[49] The Clause thus prohibits both traditional penalties and "newfangled ways to punish disfavored individuals or groups."[50]

a. Under the Functional Test, the SEA's Burdens Imposed by the SEA Exceed Any Non-Punitive Purpose the Act Serves.

The functional test asks whether the law, "viewed in terms of the type and severity of burdens imposed, reasonably can be said to further nonpunitive legislative purposes."[51] "In

---

45 *Id.* (citation omitted).

46 SEA § 2(a)(2).

47 *Cummings v. Missouri*, 71 U.S. 277, 320 (1866).

48 *Kaspersky Lab v. U.S. Dep't of Homeland Sec.*, 909 F.3d 446, 455 (D.C. Cir. 2018) (quotations omitted).

49 *Id.* (citation omitted).

50 *Id*. at 454 (citation omitted).

51 *Nixon*, 433 U.S. at 475–76 (citations omitted).

short: identify the purpose, ascertain the burden, and assess the balance between the two."[52] To determine whether the statute goes farther than necessary, courts compare the burden actually imposed with "less burdensome alternatives" the legislature could have used to achieve the same objective.[53] "A statute may be less burdensome when it includes procedural safeguards to protect the constitutional and legal rights of [the] individual[s] adversely affected, lasts only temporarily or sunsets at a time certain, allows the affected individual to relieve himself of the burden by taking belated[] corrective action, or imposes conditions instead of an absolute bar."[54]

The SEA's purpose, according to its legislative history, is "to ensure [that] only trusted radio frequency devices are authorized"—specifically, to address the risks of "harmful equipment in our nation's communications networks" by "remov[ing] compromised equipment from American networks."[55] The SEA thus appears aimed at closing what has been called a "glaring loophole" in the SNA with respect to permitting privately funded Covered List equipment to be deployed in broadband networks.[56]

But the burdens the SEA imposes on Hikvision are vastly disproportionate to this goal. Indeed, because Hikvision does not make communications equipment, applying the SEA to Hikvision does not further this purpose *at all*—it simply burdens the company with no possible benefit in increased security for advanced communications service networks. For the same reasons, Congress eschewed an obvious and more tailored alternative. The most direct way to close the "loophole" was to do just that—to prohibit commercial providers of advanced communications services from using covered broadband equipment in their networks.

Indeed, limiting the SNA, and thus the SEA, by its terms to "communications equipment and service," meaning equipment and service that is essential to broadband, would implement that more-tailored alternative—at least to the extent of distinguishing peripheral devices such as Hikvision's NVRs and cameras from broadband network switches and routers. Notably, the Commission applied the reimbursement provisions of the SNA to reflect such a limitation. The Commission thus conveyed in its *Third Report and Order* that USF recipients will not be reimbursed to remove Hikvision equipment from their networks, and therefore have no legal obligation to do so.[57] And the Commission's recent FAQ on reimbursements under the SNA

---

[52] *Kaspersky Lab*, 909 F.3d at 455.

[53] *Nixon*, 433 U.S. at 482.

[54] *Kaspersky Lab*, 909 F.3d at 456 (alterations in original, quotations and citations omitted).

[55] H.R. Rep. No. 117-148, at 2 (2021).

[56] Commissioner Carr has stated, "The FCC's rules expressly allow the continued installation of this equipment, so long as federal dollars are not involved. This is a glaring loophole . . . . It is the presence of this insecure equipment in our equipment that is the threat . . . ." *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program*, Notice of Proposed Rulemaking and Notice of Inquiry, Statement of Commissioner Brendan Carr, FCC No. 21-73, ET Docket No. 21-232, 59 (rel. June 17, 2021) ("NPRM").

[57] *Supply Chain Third Report and Order* ¶¶ 38–39.

underscores that "the replacement of non-Huawei or ZTE . . . customer premises equipment [is] not reasonably necessary to the removal . . . of covered communications equipment or service," and accordingly "costs associated [with the removal of such equipment] are ineligible for reimbursement."[58]

Yet the SEA imposes a sweeping, indefinite ban of Hikvision products from the United States. A broad reading of the SEA reaching to Hikvision video surveillance equipment would prevent the future importation, marketing, and sale of all Hikvision cameras to individuals and small businesses. Because video cameras are Hikvision's most popular and important product, if the SEA and SNA statutorily reach beyond broadband network equipment, the SEA effectively puts Hikvision out of business in the United States—permanently, with no procedural safeguards and no opportunity for mitigation or escape. Few more severe punishments exist for a business. This is precisely the sort of inflexible, absolute bar that violates the Bill of Attainder Clause.[59] Furthermore, Congress imposed this punitive measure even though a less restrictive alternative was readily available.

The SEA's status as a bill of attainder is laid bare when contrasted with how Congress normally addresses companies that it thinks pose a supply chain risk. Under the FASC Security Act, also passed in 2018, any company potentially subject to an exclusion or removal order would receive notice, including the relevant procedures and basis, a chance to respond, and an avenue for judicial review.[60] Section 889 contains no similar procedures and no standards at all; it simply targets the named companies, including Hikvision—and it does so permanently.

By the same token, the SEA is also *under*-inclusive.[61] The SEA targets only the five Chinese companies included on the covered list. But it includes no other companies—Chinese or otherwise—with similar ownership, products, cybersecurity measures, or other attributes. A genuinely nonpunitive cybersecurity law would apply neutral standards to all companies to avoid both over- and under-inclusiveness, as the FASC Security Act does.

Given that less burdensome alternatives were readily available, the SEA cannot "reasonably can be said to further" the government's nonpunitive interests.[62] And to the extent the Commission's NPRM suggests that banning Hikvision's cameras is necessary to more broadly protect "the national security of the United States or the security and safety of United

---

[58] FCC, *Secure and Trusted Communications Networks Reimbursement Program: Frequently Asked Questions* at 11, https://docs.fcc.gov/public/attachments/DOC-376062A1.pdf (last updated Sept. 24, 2021).

[59] *See Kaspersky Lab*, 909 F.3d at 456.

[60] Federal Acquisition Supply Chain Security Act of 2018, Pub. L. 115-390, Title II, 132 Stat. 5173, 5181–82 (2018).

[61] *See Kaspersky Lab*, 909 F.3d at 456 (the functional test considers the law's "scope or selectivity" (citation omitted)); *Foretich*, 351 F.3d at 1224 (statute's narrow focus could not be explained "without resort to . . . punitive purposes" (citation omitted)).

[62] *See Nixon*, 433 U.S. at 475–76.

States persons,"[63] that suggestion is not credible. If the government sees no reason even to require USF recipients to remove Hikvision equipment from their networks, it cannot credibly claim that national security requires banning new Hikvision equipment from the U.S. market entirely.

b. The Historical Inquiry Also Confirms that the SEA is a Bill of Attainder.

The historical test confirms that the SEA punishes Hikvision.[64] This inquiry asks "whether the challenged statute falls within the historical meaning of legislative punishment."[65] Here, the SEA resembles three historical legislative punishments: an employment bar, banishment, and a badge of infamy.

First, the SEA is like an employment bar, i.e., a law "barring designated individuals or groups from participation in specified employments or vocations."[66] As here, Congress historically justified these measures on national security grounds.[67] But the courts have consistently recognized that these laws are in fact legislative punishment. The same logic applies here. The SEA effectively bars Hikvision from the main employment it has lawfully pursued for many years: selling video cameras to small businesses and consumers. Legally barring a camera company from selling cameras is like barring a lawyer from being a lawyer; both fall within the "mode of punishment commonly employed against those legislatively branded as disloyal."[68]

Second, the SEA resembles a banishment—a legal order "to quit a city, place, or country, for a specified period of time, or for life."[69] Banishment involves "expel[ling] the offenders from their communities or prohibit[ing] them from accessing [certain] areas . . . for employment" or "to conduct commercial transactions."[70] So too here: the SEA would effectively and indefinitely exclude Hikvision from the United States by preventing it from selling its products

---

63 NPRM ¶ 37.

64 *See Kaspersky Lab*, 909 F.3d at 455.

65 *Selective Serv. Sys. v. Minn. Pub. Int. Rsch. Grp.*, 468 U.S. 841, 852 (1984).

66 *Nixon*, 433 U.S. at 474; *see, e.g.*, *United States v. Brown*, 381 U.S. 437 (1965) (barring communists from serving as officers or employees of labor unions was punishment); *United States v. Lovett*, 328 U.S. 303 (1946) (same, for government employees).

67 *See, e.g.*, *Brown*, 381 U.S. at 453 (bill targeted "members of a political group thought to present a threat to the national security," as did "the overwhelming majority of English and early American bills of attainder").

68 *Nixon*, 433 U.S. at 474.

69 *United States v. Ju*, 198 U.S. 253, 269–70 (1905).

70 *Doe v. Miller*, 405 F.3d 700, 719 (8th Cir. 2005).

here. A consumer-products company that cannot sell its products cannot operate. As applied to Hikvision, the SEA is thus like a historical banishment.

Third, the SEA imposes a brand of disloyalty and infamy, meaning a legislative "judgment censuring or condemning" the target.[71] The SEA unmistakably conveys a legislative judgment that Hikvision is untrustworthy and dangerous—that, in the Commission's words, its products "pose an unacceptable risk to the national security of the United States or the security and safety of United States persons."[72]

c. The Legislative Record Confirms Congress's Intent to Punish Hikvision.

Finally, "the legislative record 'evinces a congressional intent to punish'" the entities on the Covered List, which currently (incorrectly) includes Hikvision.[73] The SEA's legislative history teems with legislators' (unsupported) assertions that the listed companies will prey upon unsuspecting U.S. individuals and companies. Individual legislators described these companies, variously, as "untrusted foreign adversaries," or "Chinese companies that act on [the Chinese Communist Party's] behalf . . . compromising our telecommunications networks."[74] A representative characterized "[a]ll of these companies . . . [as] Chinese companies that are either partly or wholly owned by the Chinese Government and that have ties to the CCP."[75] The same representative implores "this body [to] do all it can to stop the undue and malign influences of the CCP from infiltrating our data and our telecommunications network."[76] Another representative added that "[w]hen foreign adversaries, like Communist China, try to prey upon these companies, they are in turn attempting to prey upon hardworking Americans like my constituents."[77]

To be sure, some of this language is about preventing supposed future harms instead of punishing specific past deeds, but the Bill of Attainder Clause is not limited to laws with retrospective focus. Indeed, historical bills of attainder were often aimed at supposed future dangers, reflecting the legislature's view "that a given person or group was likely to cause trouble . . . and therefore inflicted deprivations upon that person or group in order to keep it from

---

71 *Foretich*, 351 F.3d at 1220 (quoting *Brown*, 381 U.S. at 453–54); *see SBC Commc'ns, Inc. v. FCC*, 154 F.3d 226, n.17 (5th Cir. 1998) (noting that James Madison argued in 1794 that a formal legislative denunciation of democratic societies involved in the Whiskey Rebellion would violate the Bill of Attainder Clause).

72 NPRM ¶ 37.

73 *Selective Serv. Sys.*, 468 U.S. at 852 (quoting *Nixon*, 433 U.S. at 478).

74 167 Cong. Rec. H5655 (daily ed. Oct. 19, 2021) (statement of Rep. Pallone); *id.* (statement of Rep. Scalise).

75 *Id.* (statement of Rep. Scalise).

76 *Id*.

77 *Id.* at H5656 (statement of Rep. Pence).

bringing about the feared event."[78] Likewise, here the SEA "embodies legislative determinations that [Hikvision is] a danger to" the United States and that the company must be excluded from the country "in order to protect [it] from future harm."[79]

B. Congress Cannot Authorize the Commission to Effect an Equal Protection Violation.

We have already shown that the Commission, acting on its own, cannot violate the Fourteenth Amendment by denying equipment authorizations to companies on the basis of alienage or national origin.[80] This remains true after the passage of the SEA because the Constitution prohibits Congress from violating Hikvision's equal protection rights, just as it prohibits the Commission from doing so.[81] When Congress discriminates on the basis of national origin, its action "is presumptively invalid and will only be upheld if . . . narrowly tailored to achieve a compelling government purpose."[82] And, as we pointed out in our comments, even national security concerns do not excuse the requirement that legislation drawn along national-origin lines be narrowly tailored to survive strict scrutiny.[83] Congress cannot define a class of manufacturers solely based on their Chinese nationality and instruct the Commission to treat those companies differently than non-Chinese companies manufacturing functionally identical products, because such a broad approach lacks the narrow tailoring required.

III. THE RECORD PROVIDES NO NON-SPECULATIVE RATIONAL BASIS FOR CONCLUDING THAT HIKVISION VIDEO SURVEILLANCE EQUIPMENT POSES A UNIQUE THREAT, LET ALONE NON-VIDEO SURVEILLANCE EQUIPMENT, AND THUS THE PROPOSED REGULATIONS WOULD BE ARBITRARY AND CAPRICIOUS.

As noted above, Hikvision and its subsidiaries and affiliates produce non-video surveillance equipment and video surveillance equipment, and produce no broadband network equipment. With respect to non-video surveillance equipment, the proposed rules would be

---

78 *Brown*, 381 U.S. at 458–59.

79 *Foretich*, 351 F.3d at 1204.

80 Hikvision Comments at 65–70.

81 Technically, the Fourteenth Amendment's Equal Protection Clause applies only to the *states*, but the Court has long recognized that the Fifth Amendment's Due Process Clause includes an "equal protection component" prohibiting the federal government from discriminatory actions, and it treats "the equal protection obligations imposed by the Fifth and the Fourteenth Amendments as indistinguishable." *Adarand Constructors, Inc. v. Pena*, 515 U.S. 200, 204, 217 (1995).

82 *NAACP v. U.S. Dep't of Homeland Sec.*, 364 F. Supp. 3d 568, 576 (D. Md. 2019).

83 *See* Hikvision Comments at 67 n.181 (citing *Twitter, Inc. v. Session*, 263 F. Supp. 3d 803, 816 (N.D. Cal. 2017)).

arbitrary and capricious because they lack any foundation for treating Hikvision non-video surveillance equipment differently from other non-video surveillance equipment. With respect to video surveillance equipment, the proposed rules would be arbitrary and capricious because there is no evidence that Hikvision equipment poses a differential cybersecurity risk to its users than non-Hikvision video surveillance equipment. Hikvision equipment is frequently deployed in configurations not connected to the Internet, and even when connected to other equipment connected to the Internet, can be adequately protected just as any other video surveillance equipment—or peripheral devices, more broadly. Indeed, the MITRE Corporation's inventory of Common Vulnerabilities and Exposures ("CVEs") demonstrates that Hikvision has continued to find, disclose and patch any product vulnerabilities—practices that are comparable to those of its major competitors.[84]

A. There Is No Reason to Exclude Hikvision's Non-Video Surveillance Equipment from the SDOC Process.

The Commission's proposed regulations would require all devices produced by Hikvision and its subsidiaries and affiliates—most of which either do not intentionally emit electromagnetic radiation or do not fit within the scope of, and thus cannot possibly be included on, the Covered List—to apply for authorization through the Commission's equipment certification process, rather than through the SDOC process. There is no rational reason to require *all* equipment produced by entities with *some* equipment on the Covered List to go through that more onerous process when that equipment is clearly not video surveillance equipment. Equipment such as Hikmicro's thermal monocular, a device designed for outdoor enthusiasts to observe animals in nature, is neither telecommunications nor video surveillance equipment.[85] To group these Hikvision and Hikvision-subsidiary or affiliate devices together with telecommunications and video surveillance equipment would be arbitrary and capricious both because it would expand the Covered List beyond any possible view of Congress' intended scope, and because there is no particularized or credible evidence that this Hikvision equipment even connects to communications networks, let alone poses any unique or material cybersecurity threat either to the nation's telecommunications infrastructure or to private businesses. Thus, the burdens of the Commission's proposed rules—to the extent they include Hikvision and Hikvision-subsidiary and affiliate equipment that is not video surveillance equipment—far outweigh any unspecified and unarticulated national security benefits.

B. The Proposed Rules Are Arbitrary and Capricious Because Neither the Commission Nor Any Commenters Offered Particularized or Credible Evidence that Hikvision Video Surveillance Equipment Poses a National Security Threat.

Neither the Commission nor any commenters in this docket have identified any particularized finding, or anything beyond mere speculation, that the peripheral equipment that

---

[84] *See infra*, n.92.

[85] *See supra*, Section I.A.2.

Hikvision sells in the United States poses a threat to national security.[86] First, as set forth in Hikvision's opening comments, reply comments, and the expert report accompanying the reply, fears of Chinese espionage or third-party access to Hikvision video surveillance equipment are not only unfounded but implausible given that Hikvision video surveillance equipment can be deployed so as to have either no interface with outside networks, or limited exposure to these networks governed by enterprise-level security measures, such as firewalls, that regulate the extent to which the camera's network can communicate with outside networks. Even when an end user chooses an Internet-connected deployment, Hikvision encourages installers to set up a firewall between its network and the Internet, or to take other security measures. Indeed, as Hikvision has noted, security professionals in this docket confirm that Hikvision security cameras are often secured by a closed network, so that they never have direct access to the Internet.[87] Citing Shodan search engine results to prove the number of Hikvision Internet-connected devices in the United States is highly misleading.[88] In fact, Shodan demonstrates that only a small percentage of total Hikvision devices in the United States are accessible from the Internet.

Second, for those devices that *are* accessible from the Internet, a cybersecurity assessment of Hikvision equipment conducted by FTI confirms that the software vulnerabilities discussed in Lithuania's National Cyber Security Center report ("Lithuanian report")[89] do not exist in actual Hikvision devices.[90] While the Lithuanian report alleged that Hikvision uses software solutions with 95 common available vulnerabilities and exposures, the open-source software packages Hikvision "integrates into its camera software and firmware are encompassed

---

[86] Moreover, Hikvision equipment does not meet NTIA's multifactor analysis for making a recommendation based on national security law and enforcement concerns. *See China Telecom (Americas) Corp.*, File Nos. ITC-214-20010613-00346, ITC-214-20020716-00371, ITC-T/C-20070725-00285, Executive Branch Recommendation to the Federal Communications Commission to Revoke and Terminate China Telecom's International Section 214 Common Carrier Authorizations, at 14–15 (filed Apr. 9, 2020). As described in this section, there is no credible evidence that Hikvision video surveillance equipment poses any national security threat or that the Chinese government would be able to gain access to data from Hikvision cameras in the United States.

[87] *See* Hikvision Reply at n.164.

[88] *See* Reply Comments of IPVM at 4–5, ET Docket No. 21-232 (filed Oct. 18, 2021) ("IPVM Reply").

[89] *See* Nat'l Cyber Sec. Ctr. Under Ministry of Nat'l Def., Research & Dev. Div., *Report on the Assessment of Cyber Security of Video Surveillance Cameras Intended for Household Use* (2021), https://d1tzzns6d79su2.cloudfront.net/uploads/embedded_file/e6609d3b6aa299918f6d1ae5e3c802d57bd25cdcf7db2565baa27095e32c8af0/a94cee92-c8e6-45d0-a1ec-ef5f7dbc2761.pdf; *see also* Motorola Reply at 23–24; Comments of IPVM at 3, ET Docket No. 21-232 (filed Sept. 20, 2021).

[90] FTI Nov. 2021 Report at 4.

in a 'secure shell' and incorporate compensating controls to prevent any tampering and mitigate the publicly known vulnerabilities. FTI's vulnerability assessment scans concluded that none of the vulnerabilities present in the outdated packages were present on the devices . . . ."[91]

Third, as Hikvision has noted in both its comments and reply, the Common Vulnerabilities List, a library that tracks cybersecurity vulnerabilities and exposures launched by the MITRE Corporation and sponsored by the Department of Homeland Security Cybersecurity and Infrastructure Security Agency, shows that Hikvision has consistently disclosed vulnerabilities like the other leading video surveillance manufacturers, which Hikvision also remediated.[92] Hikvision has had only one CVE in its video surveillance equipment to date in 2021[93]—to which Hikvision disclosed the vulnerability and released patches to correct it on the same day.[94]

Finally, Hikvision's inclusion on the Department of Defense's list of Communist Chinese Military Companies pursuant to section 1237 of the National Defense Authorization Act for Fiscal Year 1999 ("CCMC List") or the Non-SDN Chinese Military-Industrial Complex Companies List ("NS-CMIC List") does not reflect a determination that Hikvision poses a cybersecurity risk to U.S. telecommunications networks or end users. The NS-CMIC List is used

---

91 *Id*.

92 Hikvision compiled the following data as of November 9, 2021 from MITRE's database:

Manufacturers	Number of Critical CVEs	Number of High CVEs	Number of Medium/Low CVEs	Total Critical/High CVEs	Total Reported CVEs
Bosch	**14**	**23**	**11**	**37**	**48**
Dahua	**8**	**18**	**6**	**26**	**32**
Axis	**3**	**22**	**14**	**25**	**39**
Hanwha/Samsung	**8**	**8**	**3**	**16**	**19**
Hikvision	**4**	**6**	**5**	**10**	**15**

93 *See* Hikvision Common Vulnerabilities and Exposures, CVE, https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=Hikvision (last visited Nov. 15, 2021).

94 *See* Hikvision, *Security Notification—Command Injection Vulnerability in Some Hikvision Products,* https://www.hikvision.com/hk/support/cybersecurity/security-advisory/security-notification---command-injection-vulnerability-in-some-/security-notification-command-injection-vulnerability-in-some-hikvision-products/ (last updated Nov. 8, 2021); Hikvision, *Important Firmware Update*, https://www.hikvision.com/hk/support/cybersecurity/security-advisory/security-notification---command-injection-vulnerability-in-some-/important-product-firmware-update/ (last visited Nov. 15, 2021).

solely for limitations on investment in publicly traded securities,[95] and although section 1237 authorizes the President to impose broader sanctions on companies on the CCMC, the Department of Defense withdrew all company designations (including of Hikvision) in June 2021.[96] Neither list is one of the specified bases for inclusion in the Covered List. Further, as Hikvision has previously made clear in its comments, it does not collect information on who its U.S. end users are or where they have located Hikvision equipment.[97] As Hikvision has explained, in the United States, it sells through a network of distributors and dealers, and does not have a general warranty registration program or other method to collect information on specific end users, and its warranties all run through its dealers.[98]

C. The Proposed Rules Are Arbitrary and Capricious Because They Ignore the Enormous Burden They Place on American Businesses and Consumers.

The Commission fails to account for the substantial cost of its proposed equipment authorization regime on American businesses and consumers. In the NPRM, the Commission claims that a "conventional cost-benefit analysis—which would seek to determine whether the costs of [its] proposed actions exceed their benefits—is not necessary"[99] because it has "no discretion" to question the decisions of other agencies on whether to place certain equipment on the Covered List.[100] Hikvision and multiple commenters in this docket disagree with the Commission's analysis, and find that because the costs of the proposed rules are likely to be immense, the Commission must conduct a cost-benefit analysis that tailors the burdens its proposed rules would impose on small businesses, end users, manufacturers, global trade agreements, and agency staff to any national security risk.[101] The Commission has authority to conduct such an analysis—recently, the Fifth Circuit confirmed the Commission's authority to

---

95 *See* U.S. Dep't of the Treasury, *Non-SDN Chinese Military-Industrial Complex Companies List*, https://home.treasury.gov/policy-issues/financial-sanctions/consolidated-sanctions-list/ns-cmic-list (last updated June 16, 2021).

96 Notice of the Removal of the Designation as Communist Chinese Military Companies Under the Storm Thurmond NDAA for FY99, 86 Fed. Reg. 33994 (June 28, 2021).

97 *See* Hikvision Comments at 58–59.

98 *Id*. at 59.

99 NPRM ¶ 79.

100 *Id*. ¶¶ 70–71.

101 *See, e.g*., Comments of CTIA at 17–18, ET Docket No. 21-232 (filed Sept. 20, 2021) ("CTIA Comments"); Comments of the Information Technology Industry Council at 12–13, ET Docket No. 21-232 (filed Sept. 20, 2021) ("ITIC Comments"); Comments of the Consumer Technology Association at 21–22, ET Docket No. 21-232 (filed Sept. 20, 2021) ("CTA Comments").

make "limited, communications-focused judgment[s]" in national security issues.[102] Further, failing to consider and assess the tremendous costs of its proposed rules would be inconsistent with recent Commission policy to conduct an informed analysis of economic issues, including an assessment of costs and benefits, "to ensure that the agency's decision is not deemed 'arbitrary and capricious.'"[103]

Despite the fact that Hikvision video surveillance equipment is peripheral devices that do not pose a cybersecurity risk to telecommunications networks in the United States,[104] the Commission's proposed rules would deprive millions of consumers—who rely on Hikvision devices for safety and health—of the ability to replace or purchase new equipment.[105] As numerous distributors of Hikvision equipment have stated in this docket, Hikvision offers high-quality and affordable video surveillance equipment, and its removal from the United States may make new video surveillance installations unaffordable to many homeowners, businesses, and organizations.[106] For small businesses, replacing Hikvision equipment would entail a significant

---

[102] *Huawei Techs. USA, Inc. v. FCC*, 2 F.4th 421, 443 (5th Cir. 2021); *see also* CTIA Comments at 17 n.43; CTA Comments at 22.

[103] Memorandum from Thomas M. Johnson, Jr., General Counsel, Office of General Counsel and Giulia McHenry, Chief, Office of Economics and Analytics, to FCC Bureau and Office Chiefs, at 6 (Nov. 19, 2020), https://docs.fcc.gov/public/attachments/DOC-368271A1.pdf.

[104] *See* CTIA Comments at 18 (stating that "network equipment poses much different national security risks than consumer end devices, yet the NPRM treats them all equally").

[105] *See* Hikvision Reply at 48–49; *see also, e.g.,* CTA Comments at 14; CTIA Comments at 10; Comments of Dahua Technology USA Inc. at 5, ET Docket No. 21-232 (filed Sept. 20, 2021).

[106] *See, e.g.,* Comments of Yisrael Gold, ET Docket No. 21-232 (filed Aug. 24, 2021) (describing how the quality and price of Hikvision cameras are superior to those of other manufacturers); Comments of Stu Forchheimer, ET Docket No. 21-232 (filed Sept. 16, 2021) ("Forchheimer Comments") (describing Hikvision's equipment as "some of the most effective cameras on the market at a price point that allows us to meet budget requirements that provide some of the best images allowing us to provide quality video to the authorities that will use the video for actionable results"); Comments of Don Kwapien, ET Docket No. 21-232 (filed Sept. 21, 2021) (noting the affordable pricing and technological innovation of Hikvision's security cameras); Comments of Scott Joyce, ET Docket No. 21-232 (filed Sept. 20, 2021) (stating that Hikvision's "product choices are vast, easy to use, inexpensive, and extremely reliable" and "have features that are unavailable from non[-]Chinese companies such [as] full color in total darkness"); Comments of Faisal Farooqui, ET Docket No. 21-232 (filed Sept. 20, 2021) (stating that other than Hikvision, it is impossible "to find a compliant system that meets those client needs which have all the features they want at a cost they [can] afford"); Comments of Anthony DeStefano, ET Docket No. 21-232 (filed Sept. 20, 2021) (stating that Hikvision's "very affordable product makes it possible to install video cameras in areas that at one time would not make it economic sense"); Comments of Mark

undertaking that could take years to complete due to the tremendous existing pandemic-induced backlog in the video surveillance industry, and leave them with substantial unusable inventory.[107] Any suggestions that there are forty manufacturers ready to assume Hikvision's place in the United States video surveillance market[108] contemplate such a rip-and-replace approach—which would be highly disruptive to American businesses and consumers—and are inaccurate. In fact, numerous security professionals disagree with this claim and confirm that there is no current replacement for Hikvision products on the market.[109]

Further, Hikvision has previously noted that the few commenters in this docket who support the Commission's proposed equipment authorization rules appear to base their support on the self-interested objective of removing competition from the video surveillance market rather than substantiated security claims.[110] Notably, IPVM cites the President of Uniview, a Chinese video surveillance competitor, describing the scrutiny and potential ban of Hikvision equipment as "an opportunity for Uniview."[111] Similarly, China Tech Threat claims that

---

Crumbacher, ET Docket No. 21-232 (filed Sept. 20, 2021) (noting that the "loss of Hikvision" would impose significant costs on his customers); Comments of Joe Polizzi, ET Docket No. 21-232 (filed Aug. 30, 2021) (stating that "[i]f Hikvision we[re] to be removed from the US market[,] a huge, unfillable, gap would be created in the security market. Costs and lead times would skyrocket[,] leaving our customers less secure").

[107] *See* Hikvision Reply at 45–46; *see also* Forchheimer Comments ("Removing [Hikvision] will cause a supply problem in our industry that would be 10X worse than any Pandemic we have seen or any other event that can affect a supply chain of this magnitude. It would cripple our business and the industry as a whole. Video surveillance would only be available for the wealthiest institutions. . . . We are having difficulties acquiring [Hikvision] product[s] now, removing the ability to acquire [these] product[s] during the [p]andemic will halt our video surveillance installation business."); Comments of James M Starr, ET Docket No. 21-232 (filed Sept. 16, 2021) ("Starr Comments") ("The replacement of [Hikvision and Dahua] equipment will be an incredible undertaking that will take years to complete due to a current lack of a viable replacement or the current manufacturing volume by competitors to Hikvision/Dahua."); Comments of Michael Edwards, ET Docket No. 21-232 (filed Sep 20, 2021) ("Removing [Hikvision] from our authorized products to sell would create dead inventory that we would not be able to sell and would cause financial hardship at a time when we are still working hard to make it out of the COVID disruption."); Comments of Ciprian Pasare, ET Docket No. 21-232 (filed Aug. 27, 2021) ("Pasare Comments") ("The decision to eliminate [Hikvision] from the US market will have a huge impact on our small business as it will be difficult to start all over again with training, testing and investing in other products on the market.").

[108] IPVM Reply at 1–2; Reply Comments of China Tech Threat at 6, ET Docket No. 21-232 (filed Oct. 18, 2021) ("China Tech Threat Reply").

[109] *See, e.g.*, Forchheimer Comments; Starr Comments; Pasare Comments.

[110] *See* Hikvision Reply at 54.

[111] IPVM Reply at 2 (citation omitted).

removing highly subsidized PRC entities from the market will allow other non-Chinese companies to enter the market.[112] It is also no surprise that Motorola—a supporter of the proposed policy change—is a direct competitor of Hikvision and stands to benefit from Hikvision's removal from the U.S. video surveillance market.

IV. THE PROPOSED REGULATIONS WOULD PLACE AN EXCESSIVE BURDEN ON COMMISSION RESOURCES.

As a practical matter, requiring manufacturers to obtain equipment authorization through the certification process,[113] instead of the more streamlined SDOC process,[114] will impose a substantial burden on Commission resources. As Hikvision has noted,[115] multiple commenters, including a coalition of trade and industry organizations, have expressed concern that the proposed equipment authorization regime would strain Commission resources by imposing additional and novel security responsibilities on the Office of Engineering and Technology ("OET").[116] Subjecting previously exempt low-emission devices to the equipment certification process would result in the Commission becoming gatekeeper for a vast number of new devices, and require an increase in staffing and the development of new areas of expertise to avoid introducing delays to the equipment review process.[117] This would be particularly burdensome as Acting Chairwoman Rosenworcel has lamented the "significant depletion of engineer staff at the Commission"[118] and that funding constraints interfere with OET's ability to address security issues.[119] Further, as CTIA notes, there is also a "well-documented shortage of cybersecurity

---

[112] China Tech Threat Reply at 5–6.

[113] *See* NPRM at App'x A (proposed § 2.907(c)).

[114] *See id*. ¶ 57.

[115] *See* Hikvision Reply at 53–54.

[116] *See id*. at n.217; Reply Comments of the Consumer Technology Association at 12, ET Docket No. 21-232 (filed Oct. 18, 2021) ("CTA Reply").

[117] Letter from ACT–The App Association, Consumer Technology Association, Council to Secure the Digital Economy, CTIA, Internet Association, Information Technology Industry Council, U.S. Chamber of Commerce, and USTelecom to Marlene H. Dortch, Secretary, FCC, ET Docket No. 21-232, at 2 (filed Sept. 20, 2021) ("Trade Associations NPRM Letter"); CTA Comments at 11.

[118] *Nominations of Jessica Rosenworcel and Ajit Pai to the FCC: Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 112th Cong. 68 (2011) (response of Jessica Rosenworcel to written questions submitted by Hon. Olympia J. Snowe).

[119] Jessica Rosenworcel, Commissioner, FCC, Statement Before the Senate Subcommittee on Financial Services and General Government, Committee on Appropriations (Mar. 10, 2020).

professionals in the United States' workforce."[120] Considerable delay to the equipment review process would interfere with the ability of companies to introduce equipment to the market, and lead them to "abandon[] new products due to the unlikelihood of timely authorization, or shift[] innovations to other markets."[121] It would also disrupt global trade practices and relationships, including mutual recognition agreements that expedite global trade of telecommunications equipment.[122] These outcomes would have a substantial adverse impact on American consumers and the economy and must be avoided.

[120] CTIA Comments at 20 (citing U.S. Gov't Accountability Off., GAO 19-144, Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs (2019) ("OMB and our prior reports have pointed out that the federal government and private industry face a persistent shortage of cybersecurity and IT professionals to implement and oversee information security protections to combat cyber threats. . . . [T]he RAND Corporation and the Partnership for Public Service have reported on a nationwide shortage of cybersecurity experts in the federal government.")).

[121] CTA Comments at 11; *see also* ITIC Comments at 10.

[122] *See* CTA Comments at 23–24; CTIA Comments at 12; Trade Associations NPRM Letter at 2; Comments of USTelecom—the Broadband Association at 6, ET Docket No. 21-232 (filed Sept. 20, 2021).

V. CONCLUSION

The Commission lacks statutory authority to adopt the proposed rules with respect to Hikvision, as none of its products are "communications equipment or service" as defined in the SNA. As such, Hikvision cannot continue to be included on the Covered List and is not subject to the Secure Equipment Act. If the SEA nonetheless did cover Hikvision's video surveillance equipment, the SEA would be an unconstitutional Bill of Attainder, and the Commission's rules implementing the SEA would be arbitrary and capricious as to Hikvision. Hikvision poses no unique threat to the cybersecurity of Americans, and all suggestions to the contrary ignore both technical reality and are unadorned speculation that cannot form the basis of reasoned rulemaking.

Sincerely,

John T. Nakahata
Timothy J. Simeone
Deepika H. Ravi
John R. Grimm
Annick M. Banoun
HARRIS, WILTSHIRE & GRANNIS LLP
1919 M Street, NW, Suite 800
Washington, DC 20036
(202) 730-1300
jnakahata@hwglaw.com

Counsel to Hikvision USA, Inc.

cc: Dana Shaffer
Paul Murray
Michael Ha
Jamie Coleman
Howard Griboff
Matt Miller
Rodney Small
Justin Faulb
William Richardson
Douglas Klein
Kelley Garcia