ORAL ARGUMENT SCHEDULED SEPTEMBER 14, 2018

Nos. 18-5176 & 18-5177

UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

KASPERSKY LAB, INC. and KASPERSKY LABS LIMITED,

Plaintiffs–Appellants,

v.

UNITED STATES DEPARTMENT OF HOMELAND SECURITY, KIRSTJEN M. NIELSEN, in her official capacity as Secretary of Homeland Security, and UNITED STATES OF AMERICA,

Defendants–Appellees.

On Appeal From the United States District Court for the District of Columbia, Nos. 1:17-cv-02697 & 1:18-cv-00325, Honorable Colleen Kollar-Kotelly

BRIEF OF APPELLANTS

Ryan P. Fayhee
Scott H. Christensen
Stephen R. Halpin III
HUGHES HUBBARD & REED LLP
1775 I Street, N.W.
Washington, D.C. 20006-2401
Telephone: (202) 721-4600
Email: ryan.fayhee@hugheshubbard.com
Email: scott.christensen@hugheshubbard.com
Email: stephen.halpin@hugheshubbard.com

Attorneys for Plaintiffs–Appellants

Certificate as to Parties, Rulings Under Review, and Related Cases

Pursuant to D.C. Circuit Rule 28(a)(1), Appellants Kaspersky Lab, Inc. and Kaspersky Labs Limited state as follows:

(A) Parties and Amici

Appellants in this case are Kaspersky Lab, Inc. and Kaspersky Labs Limited (collectively, "Kaspersky Lab"). Appellees are the United States Department of Homeland Security, Kirstjen M. Nielsen, in her official capacity as Secretary of Homeland Security (both defendants in Case No. 1:17-cv-02697 (CKK)), and the United States of America (the defendant in Case No. 1:18-cv-00325 (CKK)).

(B) Rulings Under Review

Appellants seek review of the orders and consolidated memorandum opinion of District Judge Colleen Kollar-Kotelly entered on May 30, 2018, granting the motions to dismiss filed by Appellees below (Docket Entries 25 & 26 in Case No. 1:17-cv-02697 (CKK) and Docket Entries 13 & 14 in Case No. 1:18-cv-00325 (CKK)). J.A. 169–223 (memorandum opinion); *Kaspersky Lab, Inc. v. U.S. Dep't of Homeland Sec.*, Nos. 1:17-cv-02697, 1:18-cv-00325 (CKK), 2018 WL 2433583 (D.D.C. May 30, 2018).

(C) Related Cases

Appellants are not aware of any cases related to this appeal.

Corporate Disclosure Statement

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, Appellants Kaspersky Lab, Inc. and Kaspersky Labs Limited state as follows:

1. Kaspersky Lab, Inc. is a Massachusetts corporation with its principal place of business in Woburn, Massachusetts. Kaspersky Lab, Inc. is a direct wholly owned subsidiary of Kaspersky Labs Limited, a U.K. holding company.

2. Kaspersky Labs Limited has no parent corporation, and no publicly held corporation owns 10% or more of its stock.

Table of Contents

Page

Table of Contents
(continued)

Page

Table of Contents
(continued)

Page

Table of Authorities

Page(s)

Cases

---

* Authorities upon which Kaspersky Lab chiefly relies are marked with asterisks.

Table of Authorities
(Continued)

Page(s)

Table of Authorities
(Continued)

Page(s)

Table of Authorities
(Continued)

Page(s)

Table of Authorities
(Continued)

Page(s)

Administrative and Executive Materials

Other Authorities

Glossary

BOD	Binding Operational Directive 17-01, dated September 13, 2017
NDAA	National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91

Jurisdictional Statement

This Court has jurisdiction over the appeal under 28 U.S.C. §§ 1291 and 1294(1). On May 30, 2018, the District Court entered orders granting the motions to dismiss in the two underlying actions (case nos. 1:17-cv-02697 & 1:18-cv-00325), and in each order stated: "This is a final, appealable order." J.A. 137, 167. Kaspersky Lab filed notices of appeal on June 6, 2018. *Id.* at 224. Kaspersky Lab also filed an emergency motion to expedite the appeal, which this Court granted on June 12, 2018.

Statement of the Issues Presented for Review

1. "[A] law is prohibited under the bill of attainder clause 'if it (1) applies with specificity, and (2) imposes punishment.'" *Foretich v. United States*, 351 F.3d 1198, 1217 (D.C. Cir. 2003) (quoting *BellSouth Corp. v. FCC*, 162 F.3d 678, 683 (D.C. Cir. 1998)); *see* U.S. Const. art. I, § 9. Section 1634(a) of the National Defense Authorization Act for Fiscal Year 2018 (the "NDAA") applies with specificity to Kaspersky Lab and permanently prohibits it from providing any products or services to the U.S. Government. The Senator who submitted the amendment to the NDAA that became Section 1634(a) called Kaspersky Lab a "threat to our national security," J.A. 158, stated that "[t]he case against Kaspersky Lab is overwhelming," *id.* at 162, and warned that "Congress

has serious doubts about the company," *id.* at 156. Did the District Court err by concluding that Section 1634(a) is not a bill of attainder?

2. Rule 12(d) of the Federal Rules of Civil Procedure prohibits a district court from considering "matters outside the pleadings" in resolving a motion to dismiss under Rule 12(b)(6). The District Court judicially noticed—for the truth of the assertions therein—statements and documents from the Department of Homeland Security's administrative record regarding Binding Operational Directive 17-01 (Sept. 13, 2017) (the "BOD") (from case no. 1:17-cv-02697 under the Administrative Procedure Act) (the "APA Case"). The District Court adopted those judicially noticed assertions as findings of fact and, based on the findings, concluded that Kaspersky Lab did not state a plausible claim for relief in its separate case alleging that Section 1634(a) is an unconstitutional bill of attainder (case no. 1:18-cv-00325) (the "Bill of Attainder Case"). Did the District Court err by relying on material outside the complaint from a case about agency action to decide a motion to dismiss in a separate case concerning congressional action?

3. The District Court dismissed for lack of standing Kaspersky Lab's substantive and procedural claims in the APA Case after concluding the dismissal of the Bill of Attainder Case precluded redress. If the District Court erred in dismissing the Bill of Attainder Case, did it err in dismissing the substantive APA

claim? Whether or not the District Court erred in dismissing the Bill of Attainder Case, did it err in dismissing the procedural APA claim?

Statement of the Case

Relevant Facts

Kaspersky Lab is a multinational cybersecurity company exclusively focused on protecting its clients against cyberthreats, no matter their origin. J.A. 142 ¶ 18. It is one of the world's largest privately owned cybersecurity companies. *Id.* This case is about whether the legislative and executive branches of the federal government may, without due process, single out and target Kaspersky Lab by indefinitely prohibiting the federal government from using its products and services. The prohibitions in the NDAA and the BOD targeting Kaspersky Lab and all of its products, software, hardware, and services throughout the federal government are causing Kaspersky Lab irreparable harm, including substantial reputational harm. That harm will not end without relief from this Court.

The NDAA

On July 27, 2017, Senator Jeanne Shaheen proposed an amendment to the NDAA that prohibited the United States Government from using "any hardware, software, or services" from Kaspersky Lab. S. Amend. 663 to H.R. 2810, 115th Cong. (2017). In support of this amendment, Senator Shaheen publicized that Kaspersky Lab is "a threat to our national security" and "a wider threat" than

Russia's interference in a presidential election. *See* J.A. 158. Senator Shaheen claimed that the federal government's use of Kaspersky Lab software was "already a huge breach of national security data," *see id.*, and "Congress has serious doubts about the company," *see id.* at 156. Senator Shaheen issued a press release claiming that "[t]he case against Kaspersky Lab is overwhelming," and that use of its products and services on federal computers poses a "real vulnerability to our national security." *Id.* at 162.

On December 12, 2017, Congress passed the NDAA, including Senator Shaheen's amendment. Sections 1634(a) and (b) single out Kaspersky Lab and prohibit the federal government from using its software, hardware, and services. Those subsections state, in pertinent part:

> SEC. 1634. PROHIBITION ON USE OF PRODUCTS AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB.
>
> (a) Prohibition.—No department, agency, organization, or other element of the Federal Government may use, whether directly or through work with or on behalf of another department, agency, organization, or element of the Federal Government, any hardware, software, or services developed or provided, in whole or in part, by—
>
> (1) Kaspersky Lab (or any successor entity);
>
> (2) any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or
>
> (3) any entity of which Kaspersky Lab has majority ownership.

> (b) Effective Date.—The prohibition in subsection (a) shall take effect on October 1, 2018.

National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91.

The BOD

On September 13, 2017, before the passage of the NDAA and without prior opportunity for public comment, the Department of Homeland Security issued Binding Operational Directive 17-01, which required all federal departments and agencies to identify all "Kaspersky-branded products" within 30 days. *See* National Protection and Programs Directorate; Notification of Issuance of Binding Operational Directive 17-01 and Establishment of Procedures for Responses, 82 Fed. Reg. 43,782, 43,783 (Sept. 19, 2017). The BOD provided that, within 90 days, all federal departments and agencies were required to begin removing all Kaspersky-branded products from federal systems. *See id.* The Department of Homeland Security finalized the BOD on December 6, 2017. J.A. 126–29.

Procedural History

Kaspersky Lab filed two lawsuits. On December 18, 2017, Kaspersky Lab filed the first civil action against the Department of Homeland Security and its Secretary challenging the BOD, then already in effect, under the Administrative Procedure Act, 5 U.S.C. § 706(2)(A) & (B) (case no. 1:17-cv-02697). J.A. 1. Kaspersky Lab alleged a deprivation of a constitutionally protected right and

"constitutionally insufficient procedures attendant upon that deprivation." *Id.* at 21 ¶ 85.

On February 12, 2018, Kaspersky Lab filed the second civil action against the U.S. government seeking invalidation of Section 1634(a) of the NDAA (case no. 1:18-cv-00325) (the "Bill of Attainder Complaint"), which is set to take effect October 1, 2018. *Id.* at 138–39 ¶¶ 1–2.[1] Kaspersky Lab alleged that Section 1634(a) is an unlawful bill of attainder, prohibited under Article I, Section 9 of the U.S. Constitution. *See id.* at 142–49 ¶¶ 18–44.

On February 16, 2018, the District Court ordered an expedited briefing schedule on dispositive motions in the APA Case in lieu of entertaining a motion for preliminary injunction. *See id.* at 168; *id.* at 190 & n.4. That same day, the District Court also consolidated the two cases for the purpose of briefing and deciding dispositive motions. *Id.* at 168.

---

1. On June 15, 2018, after this Court granted Kaspersky Lab's unopposed emergency motion to expedite this appeal, the Department of Defense, the General Services Administration, and the National Aeronautics and Space Administration published a federal register notice—without prior opportunity for public comment—directing implementation of Section 1634(a) of the NDAA, effective July 16, 2018. *See* Federal Acquisition Regulation; Use of Products and Services of Kaspersky Lab, 83 Fed. Reg. 28,141 (June 15, 2018). That action prompted Kaspersky Lab to file, concurrent with this brief, an emergency motion to stay.

On February 22, 2018, Kaspersky Lab filed a motion for summary judgment under Rule 56 of the Federal Rules of Civil Procedure on the administrative record in the APA Case. On March 26, 2018, the Department of Homeland Security and its Secretary responded with a cross-motion for summary judgment on the administrative record and motion to dismiss pursuant to Rule 12(b)(1) of the Federal Rules of Civil Procedure. On March 26, 2018, the U.S. government also filed a motion to dismiss the complaint in the Bill of Attainder Case pursuant to Rule 12(b)(6).[2]

Rulings Presented for Review

On May 30, 2018, the District Court issued a consolidated memorandum opinion. *Kaspersky Lab, Inc. v. U.S. Dep't of Homeland Sec.*, Nos. 1:17-cv-02697, 1:18-cv-00325 (CKK), 2018 WL 2433583 (D.D.C. May 30, 2018). The District Court dismissed the Bill of Attainder Case for failure to state a claim on which relief could be granted under Rule 12(b)(6). J.A. 223. It dismissed the APA Case for lack of standing under Rule 12(b)(1). *Id.*

---

2. The government noted in the Bill of Attainder Case that "courts may take judicial notice of matters of a general public nature . . . without converting the motion to dismiss into one for summary judgment." Mem. in Supp. of Def.'s Mot. to Dismiss 3 n.1 (Docket Entry 10) (quoting *Kounty v. Martin*, 530 F. Supp. 2d 84, 89 (D.D.C. 2007)), *Kaspersky Lab, Inc. v. United States*, 1:18-cv-00325 (CKK). The government made no further effort to pursue a request for judicial notice.

The District Court's memorandum opinion includes more than 60 citations across 18 pages reciting "facts" from the Department of Homeland Security's administrative record in the APA Case. The District Court claimed that Rule 12(b)(6) allowed it to judicially notice "facts in the public record" and noted that "[t]he Court has taken judicial notice of all of the public records discussed in this Opinion." *Id.* at 191 & n.5. The District Court thus assumed the truth of all the evidence cited from the BOD administrative record. The court then used those "facts" as the basis for concluding that the Bill of Attainder Complaint should be dismissed as a matter of law for failure to state a claim upon which relief could be granted. The District Court took this extensive judicial notice without providing the parties any notice or opportunity to be heard, and concluded that oral argument "would not be of assistance in rendering a decision." *See id.* at 171–72 nn.1–2.

The District Court held that Section 1634(a) of the NDAA does not constitute a bill of attainder even though Kaspersky Lab "is prevented from seeking discretionary contracts from the United States federal government." *Id.* at 197. According to the District Court, "[a] statute that does not apply to any individual but instead deprives a large multinational corporation of one of its many sources of revenue does not threaten anyone's personal rights or freedoms." *Id.*

According to the District Court, a legislative action that can be viewed as having some nonpunitive rationale cannot be punitive or a bill of attainder. "These

provisions of the NDAA serve a legitimate and eminently reasonable nonpunitive function: protecting the United States government's information systems from the threat of Russian cyber-intrusion. This is a prospective, risk-prevention function that is distinct from punishment." *Id.* at 202.

The District Court acknowledged that the "determination that Kaspersky Lab products present a risk to [the U.S.] federal government networks" bears "the imprimatur of government authority." *Id.* at 222 (internal quotation marks omitted). Nevertheless, the District Court found that Section 1634(a) does not prevent Kaspersky Lab "from operating as a cybersecurity business." *Id.* at 197. "The company may still operate and derive revenue throughout the world, including in the United States, by selling its products to individuals, private companies, and other governments." *Id.*; *see id.* at 200 (Kaspersky Lab has been deprived of "one tiny source of revenue"). The District Court concluded that its dismissal of the Bill of Attainder Case precluded Kaspersky Lab from establishing standing in the APA Case. *Id.* at 215–16.

Summary of Argument

The District Court erred by dismissing Kaspersky Lab's complaints in the Bill of Attainder and APA Cases. Section 1634(a) of the NDAA is a bill of attainder because it singles out Kaspersky Lab for punishment. The statute is consistent with historical forms of punishment, does not rest on sufficient

nonpunitive purposes, and evinces a congressional intent to punish. The District Court misapplied Supreme Court and D.C. Circuit precedent in concluding that Kaspersky Lab failed to state a claim upon which relief could be granted in the Bill of Attainder Case. The District Court also erred in dismissing the Bill of Attainder Case by relying on evidence from the Department of Homeland Security's administrative record, which was itself the product of severe procedural deficiencies, including the lack of a right to notice and a meaningful opportunity to be heard.

The District Court erred in dismissing Kaspersky Lab's APA claims based on its erroneous dismissal of the Bill of Attainder Case. Kaspersky Lab plausibly alleged concrete and discrete injury caused by the Department of Homeland Security's issuance of the BOD that would be redressed by a favorable court decision. The District Court also erred by ignoring Kaspersky Lab's procedural due process allegation, which is predicated on lack of notice and a meaningful opportunity to be heard before the BOD's issuance, as well as deficient postdeprivation procedures.

Argument

I. Section 1634(a) of the NDAA is a bill of attainder, and the District Court erred in concluding otherwise.

Kaspersky Lab contends that Section 1634(a) of the NDAA is an unconstitutional bill of attainder. This Court reviews that constitutional challenge de novo. *Am. Bus. Ass'n v. Rogoff*, 649 F.3d 734, 737 (D.C. Cir. 2011).

A. The Bill of Attainder Clause applies to corporations.

Article I, Section 9 of the U.S. Constitution provides: "No Bill of Attainder or ex post facto Law shall be passed." The Second Circuit has held "that corporations *must* be considered 'individual[s]' that may not be singled out for punishment under the Bill of Attainder Clause." *Consol. Edison Co. of N.Y. v. Pataki*, 292 F.3d 338, 349 (2d Cir. 2002) (emphasis added) (quoting *Nixon v. Adm'r of Gen. Servs.*, 433 U.S. 425, 468 (1977)).[3] No federal court of appeals, including this Court, has held to the contrary. *See BellSouth Corp. v. FCC*, 162

3. *Consolidated Edison* involved a challenge under Article I, Section 10 of the U.S. Constitution, which prohibits the States from "pass[ing] any Bill of Attainder." 292 F.3d at 342–43. The distinction between that clause and the federal analog makes no difference. *See Fowler Packing Co. v. Lanier*, 844 F.3d 809, 816 n.5 (9th Cir. 2016) ("We see no reason . . . why the same term should be treated differently when applied to state legislatures, at least in the context of this case."); *cf. Walker v. R.J. Reynolds Tobacco Co.*, 734 F.3d 1278, 1287 (11th Cir. 2013) ("Our analysis is the same under either clause because 'the reaches of the [Due Process Clauses of the] Fourteenth and Fifth Amendments are coextensive.'" (alteration in original) (quoting *Rodriguez–Mora v. Baker*, 792 F.2d 1524, 1526 (11th Cir. 1986)).

F.3d 678, 684 (D.C. Cir. 1998) ("*BellSouth II*") (assuming that "the Bill of Attainder Clause protects corporations as well as individuals" (quoting *BellSouth Corp. v. FCC*, 144 F.3d 58, 63 (D.C. Cir. 1998) ("*BellSouth I*")).[4]

The Supreme Court has never squarely addressed whether the protections of the Bill of Attainder Clause extend beyond individual persons, but the weight of its authorities supports the proposition that the Clause—like other constitutional protections—shields corporate entities (such as Kaspersky Lab), groups, organizations, and other nonnatural persons, in addition to individuals.[5] The Bill

---

4. *See Fowler Packing Co.*, 844 F.3d at 817 ("[W]e assume without deciding that corporations may seek the protection of the Bill of Attainder Clauses—a proposition not yet endorsed by this circuit."); *SBC Commc'ns, Inc. v. FCC*, 154 F.3d 226, 234 n.11 (5th Cir. 1998) (It "does seem likely" that "the Bill of Attainder Clause applies to corporations."); *see also Planned Parenthood of Cent. N.C. v. Cansler*, 877 F. Supp. 2d 310, 314–15, 321–25 (M.D.N.C. 2012) (law that singled out Planned Parenthood Inc. and its affiliated organizations was unconstitutional bill of attainder).

5. *See Burwell v. Hobby Lobby Stores, Inc.*, 134 S. Ct. 2751, 2768 (2014) ("A corporation is simply a form of organization used by human beings to achieve desired ends."); *Citizens United v. Fed. Election Comm'n*, 558 U.S. 310, 343 (2010) ("The Court has . . . rejected the argument that political speech of corporations or other associations should be treated differently under the First Amendment simply because such associations are not 'natural persons.'" (citations omitted)); *see also Metro. Life Ins. Co. v. Ward*, 470 U.S. 869 (1985) (equal protection); *Helicopteros Nacionales de Colombia v. Hall*, 466 U.S. 408 (1984) (due process); *Penn Cent. Transp. Co. v. New York City*, 438 U.S. 104 (1978) (takings); *Marshall v. Barlow's, Inc.*, 436 U.S. 307 (1978)

(Footnote continued on next page)

of Attainder Clause protects Kaspersky Lab from unconstitutional legislative punishment.

B. Section 1634(a) punishes Kaspersky Lab.

"[A] law is prohibited under the bill of attainder clause 'if it (1) applies with specificity, and (2) imposes punishment.'" *Foretich v. United States*, 351 F.3d 1198, 1217 (D.C. Cir. 2003) (quoting *BellSouth II*, 162 F.3d at 683). Courts reviewing whether a legislative act constitutes an unlawful bill of attainder conduct a three-part inquiry, asking:

> (1) whether the challenged statute falls within the historical meaning of legislative punishment [the "historical test"]; (2) whether the statute, "viewed in terms of the type and severity of burdens imposed, reasonably can be said to further nonpunitive legislative purposes" [the "functional test"]; and (3) whether the legislative record "evinces a congressional intent to punish" [the "motivational test"].

Selective Serv. Sys. v. Minn. Pub. Interest Research Grp., 468 U.S. 841, 852 (1984) (quoting *Nixon*, 433 U.S. at 473, 475–76). Properly considered, all three tests point to the conclusion that Section 1634(a) punishes Kaspersky Lab.

(Footnote continued from previous page)

(searches and seizures); *United States v. Martin Linen Supply Co.*, 430 U.S. 564 (1977) (double jeopardy).

1. The District Court misapplied the historical test, because Section 1634(a) is consistent with historical forms of punishment.

"When our Constitution and Bill of Rights were written, our ancestors had ample reason to know that legislative trials and punishments were too dangerous to liberty to exist in the nation of free men they envisioned. And so they proscribed bills of attainder." *United States v. Lovett*, 328 U.S. 303, 318 (1946). Congress violates the Bill of Attainder Clause when it "exercises the powers and office of judge," "pronounces upon the guilt of the party, without any of the forms or safeguards of trial," "determines the sufficiency of the proofs produced, whether conformable to the rules of evidence or otherwise," and "fixes the degree of punishment in accordance with its own notions of the enormity of the offence." *Cummings v. Missouri*, 71 U.S. (4 Wall.) 277, 323 (1867). The Framers of our Constitution added the Bill of Attainder Clause to protect against a trial by Congress in the court of public opinion.

As the Supreme Court has observed, "the Bill of Attainder Clause was not to be given a narrow historical reading . . . , but was instead to be read in light of the evil the Framers had sought to bar: legislative punishment, *of any form or severity*, of specifically designated persons or groups." *United States v. Brown*, 381 U.S. 437, 447 (1965) (emphasis added) (citation omitted). "[T]he prohibition against bills of attainder has evolved far beyond the original context of capital sentences,"

but "it continues to focus on legislative enactments that 'set[] a note of infamy' on the persons to whom the statute applies." *Foretich*, 351 F.3d at 1220 (quoting *SBC Commc'ns, Inc. v. FCC*, 154 F.3d 226, 235 (5th Cir. 1998)).

a. Section 1634(a) singles out and targets Kaspersky Lab.

Specificity alone does not render a statute an unlawful bill of attainder. *See BellSouth I*, 144 F.3d at 63 (citing *Nixon v. Adm'r of Gen. Servs.*, 433 U.S. 425, 471 n.33 (1977)). But the Supreme Court's early cases "demonstrate that a statute will be particularly susceptible to invalidation as a bill of attainder where its effect is to mark specified persons with a brand of infamy or disloyalty." *Foretich*, 351 F.3d at 1219 (citation omitted).[6] Indeed, "narrow application of a statute to a specific person or class of persons raises suspicion, because the Bill of Attainder Clause is principally concerned with '[*t*]*he singling out* of an individual for legislatively prescribed punishment.'" *Id.* at 1224 (quoting *Selective Serv. Sys.*, 468 U.S. at 847); *see* Laurence H. Tribe, *American Constitutional Law* § 10-4, at 646 n.25 (2d ed. 1988) ("The identification of an individual by name should raise

6. *See also BellSouth I*, 144 F.3d at 72 (Sentelle, J., dissenting) ("[T]he very specificity of the statute would mark it as punishment, for there is rarely any valid reason for such narrow legislation; and normally the Constitution requires Congress to proceed by general rulemaking rather than by deciding individual cases." (quoting *Nixon*, 433 U.S. 425 at 486 (Stevens, J., concurring)).

an almost conclusive presumption of constitutionally suspect specification, given that the ban on bills of attainder is designed to prevent trial by legislature.").

Here, the government has never disputed that Section 1634(a) of the NDAA singles out Kaspersky Lab, and with good reason. Section 1634(a), titled "PROHIBITION ON USE OF PRODUCTS AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB," explicitly names Kaspersky Lab, and permanently forbids every "department, agency, organization, or other element of the Federal Government" from using "any hardware, software, or services developed or provided, in whole or in part" by the company or its affiliates. The statute's singling out of Kaspersky Lab is sweeping. It captures not only Kaspersky Lab itself, but "any successor entity," "any entity that controls, is controlled by, or is under common control with Kaspersky Lab," and "any entity of which Kaspersky Lab has majority ownership."

Section 1634(a) adjudges Kaspersky Lab unfit for providing goods and services to the federal government, rather than "set[ting] forth a generally applicable rule decreeing that any person who commits certain acts or possesses certain characteristics" is precluded from doing so. *See Brown*, 381 U.S. at 450. The surgical precision with which Section 1634(a) targets Kaspersky Lab and any related entities—but no others—"raises suspicion" under this Court's bill of attainder jurisprudence. *See Foretich*, 351 F.3d at 1224.

b. Section 1634(a) brands Kaspersky Lab with infamy and disloyalty.

Section 1634(a) singles out Kaspersky Lab for punishment by stamping it with Congress's legislative conclusion that the company is disloyal to the United States, or at least undeserving of the federal government's trust.[7] *United States v. Brown*, 381 U.S. 437 (1965), is instructive. There, the Supreme Court invalidated a law as an unconstitutional bill of attainder in part because it "inflict[ed] its deprivation upon the members of a political group *thought to present a threat to the national security*," rather than "establish[ing] an objective standard of conduct." *Id.* at 453–54 (emphasis added). The relevant statutory provisions in *Brown* identified "members of the Communist Party" as a shorthand for persons deserving of exclusion from labor union offices, instead of outlining statutory proscriptions in general terms and "leav[ing] to courts and juries the job of deciding what persons have committed the specified acts or possess the specified characteristics." *Id.* at 450.

Here, Congress has prohibited the use of Kaspersky Lab products and services on government systems because it considered, without a judicial

---

7. *See Little v. City of North Miami*, 805 F.2d 962, 966 (11th Cir. 1986) (public censure is "a recognized mode of punishment in certain circumstances" (footnote omitted)).

determination of guilt or blameworthiness, that Kaspersky Lab products and services create an "alarming national security vulnerability." *See* J.A. 156. There is no other explanation for the prohibition. Implicit in Section 1634(a) is Congress's judgment that Kaspersky Lab has committed such acts or possesses such characteristics that render it permanently unsuitable as a provider of products and services to the federal government. While "Congress undoubtedly possesses power" to legislate in the interest of national security, that power is not absolute and does not exempt it from enacting laws of general applicability. *See Brown*, 381 U.S. at 449–50 (Congress exceeded its power under the Commerce Clause by singling out members of the Communist Party for punishment).

This Court's decision in *Foretich* further supports a finding that Section 1634(a) brands Kaspersky Lab with infamy and further illustrates the dangers of legislative circumvention of the due process safeguards provided by the judicial branch. The plain text of the statute at issue in *Foretich* made no mention of Dr. Foretich himself or the long-running custody battle involving his former wife and daughter. Instead, Congress tracked the particular factual circumstances of the saga without regard to specific persons or the prior custody battles that had unfolded in the D.C. courts. *See Foretich v. United States*, 351 F.3d 1198, 1207 D.C. Cir. 2003). This Court nonetheless concluded that "Congress determined that

Dr. Foretich [was] a criminal child abuser," *id.* at 1226, and that the statute burdened him with "the opprobrium of being branded" as such, *id.* at 1220.

In other words, the circumspect statutory text in *Foretich* was sufficient for this Court to conclude that Congress had "singl[ed] out Dr. Foretich as virtually the only parent subject to the Act," such that "Congress has permanently associated him with criminal acts of child sexual abuse," even though the statute never mentioned Dr. Foretich by name or included any findings that he had in fact abused his daughter. *See id.* at 1223. It follows that Section 1634(a) of the NDAA—which singles out Kaspersky Lab by name against the backdrop of unsubstantiated rumors that Kaspersky Lab is a willing (or unwilling) conduit for Russian cyberattacks—has marked Kaspersky Lab with a "brand of infamy or disloyalty." *See id.* at 1219; *see also* J.A. 222 (The "determination that Kaspersky Lab products present a risk to [the U.S.] federal government networks" bears "the imprimatur of government authority" (internal quotation marks omitted)). Without any judicial process, Congress has branded one of the world's leading cybersecurity firms a cyberthreat.

c. Section 1634(a) is consistent with historical forms of punishment.

The Supreme Court has recognized "a ready checklist of deprivations and disabilities so disproportionately severe and so inappropriate to nonpunitive ends that they unquestionably have been held to fall within the proscription of Art. I,

§ 9." *Nixon v. Adm'r of Gen. Servs.*, 433 U.S. 425, 473 (1977). "[T]hose sanctions" include "imprisonment," "banishment," "the punitive confiscation of property by the sovereign," and "a legislative enactment barring designated individuals or groups from participation in specified employments or vocations, a mode of punishment commonly employed against those legislatively branded as disloyal." *Id.* at 473–74 (citations omitted). Any such enactment is "immediately constitutionally suspect," *see id.* at 473, but that does not preclude other enactments from qualifying as punishment under the historical test.

The District Court applied the historical test too narrowly. For example, it suggested that an enactment *must* fall within the checklist above to satisfy the historical test. *See* J.A. 194–95. The District Court also reasoned that because Section 1634(a) of the NDAA "targets the products of a multinational corporation," rather than individuals and their employment opportunities, "[t]he NDAA . . . is nothing like the legislation" at issue in historical bill of attainder cases. *Id.* at 196. Such observations are not faithful to the Supreme Court's precedents on historical forms of punishment and disregard the severe reputational and financial impact of broad legislative pronouncements.[8]

---

8. In *Planned Parenthood of Central North Carolina v Cansler*, 877 F. Supp. 2d 310 (M.D.N.C. 2012), the court concluded that a statute was "punitive in

(Footnote continued on next page)

Indeed, the Supreme Court's conception of historical forms of punishment encompasses more than the checklist above and other deprivations of life, liberty, or property guaranteed by the Constitution. As early as 1867, the Supreme Court rejected such a limited definition of punishment and expanded the prohibited forms of punishment to include the deprivation of other rights "known to the law":

> We do not agree with the counsel of Missouri that "to punish one is to deprive him of life, liberty, or property, and that to take from him anything less than these is no punishment at all." The learned counsel does not use these terms – life, liberty, and property – as comprehending every right known to the law. He does not include under liberty freedom from outrage on the feelings as well as restraints on the person. He does not include under property those estates which one may acquire in professions, though they are often the source of the highest emoluments and honors. *The deprivation of any rights, civil or political, previously enjoyed, may be punishment*, the circumstances attending and the causes of the deprivation determining this fact. Disqualification from office may be punishment, as in

---

(Footnote continued from previous page)

nature based on a traditional understanding of punishment," because it singled out Planned Parenthood by name for a funding ban, excluding it "from any opportunity to apply for and/or receive [North Carolina Department of Health and Human Services]-administered contracts for non-abortion-related services, which [it] had effectively provided to the public in the past." *Id.* at 324 (citation omitted). The court found "that such a categorical exclusion is analogous to legislation that prohibits a person or entity from engaging in certain employment, which courts have historically found to be associated with punishment." *Id.*

> cases of conviction upon impeachment. Disqualification from the pursuits of a lawful avocation, *or from positions of trust*, or from the privilege of appearing in the courts, or acting as an executor, administrator, or guardian, may also, and often has been, imposed as punishment.

Cummings v. Missouri, 71 U.S. (4 Wall.) 277, 320 (1867) (emphases added). Thus in *Cummings*, the Supreme Court rejected as a bill of attainder a legislative act that prohibited Confederates from serving as priests. *See id.* at 316–17.

In *Ex parte Garland*, 71 U.S. (4 Wall.) 333, 377 (1867), decided the same year, the Supreme Court rejected as a bill of attainder legislation that prohibited Confederates from being admitted to the bar and serving as attorneys. In *United States v. Lovett*, 328 U.S. 303, 315–16 (1946), the Supreme Court rejected as a bill of attainder legislation that prohibited the federal government from paying certain employees believed to be "subversives" who had been working for the government for years. The *Lovett* Court observed that "[t]his permanent proscription from any opportunity to serve the Government is punishment, and *of a most severe type*. It is a type of punishment which Congress has only invoked for special types of odious and dangerous crimes." 328 U.S. at 316 (emphasis added) (citations omitted). And in *United States v. Brown*, 381 U.S. 437, 449–50 (1965), the Supreme Court rejected as a bill of attainder legislation that made it a crime for recent members of the Communist Party to serve on the executive board of a labor organization. All of these cases have in common the deprivation of a right

previously enjoyed by a group and involved "[d]isqualification from the pursuits of a lawful avocation, or from positions of trust, . . . imposed as punishment." *Brown*, 381 U.S. at 448 (quoting *Cummings*, 71 U.S. at 320).

Among the rights protected under the Bill of Attainder Clause is the right to be free from defamation of one's reputation. In *Lovett*, the purpose of the offending legislation was to "permanently bar [respondents] from government service." 328 U.S. at 313. That bar "stigmatized their reputation and seriously impaired their chance to earn a living." *Id*. at 314. Similarly, in *Foretich*, this Court recognized that a legislative determination of criminal sexual abuse that destroyed a physician's reputation and affected his business was an unconstitutional bill of attainder, even though the statute in no way barred Dr. Foretich from practicing as a physician. 351 F.3d at 1220. The economic injury resulting from the legislature casting aspersions on a group is prohibited by the Constitution:

> [A]n official government proclamation that certain people *or groups* are dangerous subversives would "cripple the functioning and damage the reputation of *those organizations* in their respective communities and in the nation . . . [and thereby] violate each . . . *organization's* common-law right to be free from defamation." In other words, the right against defamation is a life, liberty, or property right, and neither the legislature nor the executive can violate this right without first affording due judicial process.

Anthony Dick, Note, *The Substance of Punishment Under the Bill of Attainder Clause*, 63 Stan. L. Rev. 1177, 1210 (2011) (emphases added) (quoting *Joint Anti-Fascist Refugee Comm. v. McGrath*, 341 U.S. 123, 139 (1951) (Burton, J., joined by Douglas, J.)).[9]

"Although the particular burden imposed" on Kaspersky Lab under Section 1634(a) of the NDAA "is not precisely identical to any of the burdens historically recognized as punishment," Section 1634(a) is consistent with historical forms of punishment. *See Foretich*, 351 F.3d at 1219. The historical test weighs in favor of a finding that Sections 1634(a) of the NDAA is an unconstitutional bill of attainder.

d. Cases declining to expand the category of historical punishments are distinguishable.

"[A] statute that leaves open perpetually the possibility of [overcoming a legislative restriction] does not fall within the historical meaning of forbidden legislative punishment." *BellSouth II*, 162 F.3d 678, 685 (D.C. Cir. 1998) (second alteration in original) (quoting *Selective Serv. Sys. v. Minn. Pub. Interest Research Grp.*, 468 U.S. 841, 853 (1984)). This proposition alone distinguishes Section

9. *See also Joint Anti-Fascist Refugee Comm.*, 341 U.S. at 143 (Black, J., concurring); *id.* at 161 (Frankfurter, J., concurring); *id.* at 185 (Jackson, J., concurring).

1634(a) of the NDAA from many of this Court's cases declining to find that a legislative enactment constitutes an historical form of legislative punishment.

BellSouth I concerned a statutory provision of limited duration (four years after passage), 144 F.3d 58, 61 (D.C. Cir. 1998), that was also escapable while it was in effect: "[T]he separated affiliate mechanism permit[ted] [plaintiff] to establish a wholly-owned subsidiary to pursue electronic publishing. This subsidiary could disseminate materials over the telephone lines of BellSouth's [other] subsidiaries, as long as it was kept separate from them in the ways prescribed by [statute]." *See id.* at 65. The statutory restriction "applie[d] only to electronic publishing rather than to information services as a whole, it expire[d] after five years rather than continuing indefinitely, and it mandate[d] structural separation rather than complete exclusion." *Id.* at 66.

In *BellSouth II*, the statutory restriction prevented "[certain BellSouth subsidiaries] from immediately providing in-region long distance services," 162 F.3d at 681, but the restriction could "be overcome by fulfilling [other statutory requirements]." *Id.* at 681. The entities could provide "in-region long distance services through a separate affiliate, but only after they have received the approval of the FCC by satisfying the [statutory] requirements." *Id.* at 683. In *Siegel v. Lyng*, 851 F.2d 412 (D.C. Cir. 1988), the "temporary employment bar" at issue, *id.*

at 418, was "rebuttable in adjudicatory proceedings," *id.* at 416.[10] The foregoing cases do not affect the conclusion that Section 1634(a)'s specific and permanent ban on Kaspersky Lab is consistent with historical forms of punishment.

2. The District Court misapplied the functional test, because the burden imposed by Section 1634(a) does not further nonpunitive legislative purposes.

The second step in the bill of attainder analysis—the functional test—"appears to be the most important of the three." *BellSouth I*, 144 F.3d at 65. As observed above, "[n]arrow application of a statute to a specific person or class of persons raises suspicion, because the Bill of Attainder Clause is principally concerned with '[*t*]*he singling out* of an individual for legislatively prescribed punishment.'" *Foretich*, 351 F.3d at 1224 (quoting *Selective Serv. Sys.*, 468 U.S. at 847). "Therefore, the functional test necessarily takes account of the scope or selectivity of a statute in assessing the plausibility of alleged nonpunitive purposes." *Id.* (citations omitted).

---

10. *Patchak v. Jewell*, 828 F.3d 995 (D.C. Cir. 2016), *aff'd on other grounds sub nom. Patchak v. Zinke*, 138 S. Ct. 897 (2018), which includes only a cursory bill of attainder analysis, involved a jurisdiction-stripping statute. To be sure, the enactment was permanent and lacked any means of circumventing its prohibition. This Court observed, however, that "[j]urisdictional limitations are generally not [considered a traditional form of punishment]." *See id.* at 1006 (citing *Ameur v. Gates*, 759 F.3d 317, 329 (4th Cir. 2014)).

a. Presuming a nonpunitive rationale does not make Section 1634(a) nonpunitive.

The functional test asks "whether the law under challenge, viewed in terms of the type and severity of burdens imposed, reasonably can be said to further nonpunitive legislative purposes." *Foretich*, 351 F.3d at 1220 (quoting *Nixon*, 433 U.S. at 475–76). Courts considering bill of attainder challenges cannot presume that Congress has acted rationally and without punitive purpose: the "attainder inquiry is in fact more exacting than a rational basis test, because it demands purposes that are *not merely reasonable but nonpunitive*." *BellSouth I*, 144 F.3d at 67 (emphasis added). "Punitive purposes, however rational, don't count." *Id.* And Congress's "nonpunitive aims must be 'sufficiently clear and convincing.'" *Foretich*, 351 F.3d at 1221 (quoting *BellSouth II*, 162 F.3d at 686).[11]

The fact that some nonpunitive rationale can be offered for legislation does not render the legislation nonpunitive. *See* Anthony Dick, Note, *The Substance of Punishment Under the Bill of Attainder Clause*, 63 Stan. L. Rev. 1177, 1191

---

11. The District Court observed that its role is not "to review *de novo* the technical decisions Congress makes to protect the Nation's cyber-security." J.A. 203. Instead, so long as it discerned some "rational" reason for Section 1634(a) of the NDAA, the District Court considered its inquiry complete. *See id.* The District Court thus ignored this Court's direction to conduct an inquiry that is "more exacting than a rational basis test." *See BellSouth I*, 144 F.3d at 67.

(2011) ("[L]egislatures will always be able to offer some rationale for any bill that plausibly sounds nonpunitive.").[12] In the Nineteenth Century, the legislatures purported to protect the priesthood or the rolls of attorneys from those who fought against the United States in the Civil War. *See Cummings*, 71 U.S. at 316; *Garland*, 71 U.S. 333 at 374–75. In the Twentieth Century, the legislatures purported to defend labor unions and the federal government from Communist infiltration and subversion. *See Brown*, 381 U.S. at 438–39, 453 ("[T]he purpose of [the legislation] is to protect the national economy by minimizing the danger of political strikes," which create a "threat to the national security[.]"); *Lovett*, 328 U.S. at 308 ("In the background of the statute here challenged lies the House of Representatives' feeling in the late thirties that many 'subversives' were occupying influential positions in the Government and elsewhere and that their influence must not remain unchallenged."). All of these bills of attainder sought to protect national security.

---

12. *See also* Laurence H. Tribe, *American Constitutional Law* § 10-5, at 655 (2d ed. 1988) ("[M]easures enacted not in order to punish but in order to prevent future harm have been condemned as forbidden bills of attainder when such measures have been thought to rest on a legislative determination that particular persons have shown themselves to be blameworthy or at least culpably unreliable." (citing *Brown*, 381 U.S. at 437)).

Here, the reliance on a purported national security purpose does not redeem Section 1634(a) of the NDAA and, if anything, strengthens Kaspersky Lab's case: "The temptation to utilize bills of attainder is especially strong when national security is thought to be threatened." *Linnas v. INS*, 790 F.2d 1024, 1028 (2d Cir. 1986) (citing *United States v. Lovett*, 328 U.S. 303 (1946)). Section 1634(a)'s purpose and effect are the same: to purge Kaspersky Lab from information systems based on unproven and unfounded allegations that it poses a cyberthreat. This burden functions as punishment. As the Supreme Court has made clear, Congress can pass laws of "general applicability," but cannot single out and target a specific person "upon whom the sanction it prescribes is to be levied." *Brown*, 381 U.S. at 461. Instead of Section 1634(a), Congress could have enacted a law of general applicability that would have achieved the same nonpunitive purposes.

b. The burdens Congress imposed demonstrate that Section 1634(a) is an unlawful bill of attainder.

The prohibition found in Section 1634(a) of the NDAA is complete and permanent. It leaves open no alternative means by which Kaspersky Lab or a related entity could ever provide products or services to the federal government. There is no sunset provision in the statute—it forever stains Kaspersky Lab, its successors, and its affiliates by excluding them from providing any products or services to the federal government. If Kaspersky Lab moved all of its operations

and executive leadership to Peoria, Illinois, or offered lawn-mowing services, it would still be banished from serving the federal government.

This kind of permanent exclusion from a relationship with the federal government has been stricken as an unconstitutional bill of attainder. In *United States v. Lovett*, 328 U.S. 303 (1946), the Supreme Court considered a statute that, masquerading as an appropriations bill, sought to defund the salaries of specific persons Congress suspected of subversive activities. *See id.* at 308–13. The effect of the statute was "permanently to bar [specific persons] from government service." *Id.* at 313. The Court remarked that "[t]his permanent proscription from any opportunity to serve the Government is punishment, and of a most severe type." *Id.* at 316.[13]

This Court has analyzed the type and severity of burdens imposed by Congress by comparing the affected party's status before and after the offending legislation. "Although we acknowledge that it may at times be difficult to compare a party's status before and after the enactment of regulatory legislation to

---

13. The *Lovett* Court continued that a permanent bar from government service "is a type of punishment which Congress has only invoked for special types of odious and dangerous crimes, such as treason; acceptance of bribes by members of Congress; or by other government officials; and interference with elections by Army and Navy officers." 328 U.S. at 316 (internal citations omitted).

determine whether the legislation inflicts punishment, we nonetheless believe that such a comparison is relevant to our analysis." *BellSouth II*, 162 F.3d 678, 691 (D.C. Cir. 1998). Here, Kaspersky Lab had been one of the world's largest vendors of IT security software and enterprise endpoint protection. In 2017, Kaspersky Lab scored first place in 72 out of 86 tests and reviews of its cybersecurity products. J.A. 143 ¶ 21. Now, Kaspersky Lab products and services have been branded by Congress as a threat to the security of the United States and have been ordered to be removed from government systems.[14]

Kaspersky Lab faces the prospect that the U.S. Government's unfounded mistrust of the company will remain enshrined in U.S. law. The District Court acknowledged that the "determination that Kaspersky Lab products present a risk to [the U.S.] federal government networks" bears "the imprimatur of government authority." *See id.* at 222 (internal quotation marks omitted). This reputational damage has had an immediate and severe financial impact on Kaspersky Lab, and that impact is continuing and growing. *See id.* at 149 ¶¶ 45–46. It is reasonable to infer that Kaspersky Lab's position as a trusted software vendor has been

---

14. If the Bill of Attainder Case had been allowed to proceed to discovery, Kaspersky Lab would have been able to further develop facts in support of its plausible claim that Section 1634(a) has caused and continues to cause substantial injury, distinguishable from the BOD.

compromised. And it is difficult to envision a more irreparable harm to a company's reputation than the United States Government declaring the company a threat to national security and refusing to do business with it.

c. There is a significant imbalance between the burdens Congress imposed and the purported nonpunitive purpose.

"[W]here there exists a significant imbalance between the magnitude of the burden imposed and a purported nonpunitive purpose, the statute cannot reasonably be said to further nonpunitive purposes." *Foretich v. United States*, 351 F.3d 1198, 1221 (D.C. Cir. 2003); *see also id.* at 1228 (Tatel, J., concurring) ("[E]ven though Congress had a valid nonpunitive reason for passing the [statute], it impermissibly 'piled on' an additional, entirely unnecessary burden. This punitiveness, combined with the Act's undisputed specificity, renders the Act a bill of attainder.").

Here, the purported nonpunitive purpose of "national security" cannot justify the federal government's complete and permanent ban on a single company. Rather than "clear and convincing," as the law requires, Congress's purported nonpunitive purpose is amorphous and abstract. Section 1634(a) lacks a "coherent and reasonable nexus" between the permanent, inescapable, unconditional debarment of Kaspersky Lab, and "the benefit to be gained," namely, the removal

of a supposed and unproven "threat" from federal information systems. *See id.* at 1219 (majority opinion).

Even taking into consideration and assuming the legitimacy of the threat as articulated by the government, Section 1634(a)'s singling out Kaspersky Lab for exclusion from all federal government contracting is disproportionate to that alleged threat—particularly with respect to the ban on "any . . . services." NDAA § 1634(a); *see Foretich*, 351 F.3d at 1224 ("[T]he narrow focus of the disputed Act cannot be explained without resort to inferences of punitive purpose." (internal quotation marks omitted)); *Consol. Edison Co. of New York v. Pataki*, 292 F.3d 338, 349 (2d Cir. 2002) ("When faced with a bill that is so exceptionally narrow in scope, manifestly retrospective in focus, and unavoidably punitive in operation, we cannot allow it to stand[.]"). The narrowly focused ban on Kaspersky Lab is so broad that it even precludes the federal government from relying on the company's threat intelligence and research reports, which are nonsoftware offerings that consumers do not install on any systems.

Here, as in *Consolidated Edison Co. of New York v. Pataki*, "the legislature . . . made no attempt whatsoever to ensure that the costs imposed on [the statute's target] were proportional to the problems that the legislature could legitimately seek to ameliorate." 292 F.3d at 354. There were no legislative findings or analysis relevant to the scope of Section 1634(a), but simply a congressional

mandate to impose the broadest possible ban across the entire federal government after having concluded as a matter of fact that Kaspersky Lab posed a national security threat. *See* J.A. 144–47 ¶¶ 26–37. Section 1634(a) operates as a complete ban on the Kaspersky Lab brand without any regard to proportionality.

Section 1634(a) also functions as a punishment because the magnitude of its burden is in "grave imbalance" with the purported nonpunitive purpose. *See Foretich*, 351 F.3d at 1222. To determine punitiveness, courts do not look just at the "severity of a statutory burden in absolute terms." *Id*. Rather, courts consider "the magnitude of the burden relative to the purported nonpunitive purposes of the statute." *Id*. "A grave imbalance or disproportion between the burden and the purported nonpunitive purpose suggests punitiveness, even where the statute bears some minimal relation to nonpunitive ends." *Id*. Further, the government cannot "defend the constitutionality of the statute simply by positing any nonpunitive purpose" or "purposes that superficially appear to be nonpunitive." *Id*. at 1223. Courts consider the plausibility of the government's purported nonpunitive justification, rather than accept it at face value. *Id*.

The magnitude of Section 1634(a)'s burden on Kaspersky Lab is severe. *See* J.A. 149 ¶ 45. Section 1634(a) permanently "memorializes a judgment by the United States Congress" that Kaspersky Lab deserves complete, unconditional, and permanent debarment even though executive branch officials have admitted that

there is no conclusive evidence that Kaspersky Lab has caused any breach at all. *See id*. at 147 ¶ 38; *Foretich*, 351 F.3d at 1223. This injury results from "the particular means Congress adopted in [Section 1634(a)]"—the naming and singling out Kaspersky Lab in the statute. *See Foretich*, 351 F.3d at 1223; J.A. 149 ¶¶ 45–46. In addition, beyond the reputational harm, Section 1634(a) permanently deprives Kaspersky Lab of any potential government business. J.A. 149–50 ¶ 49.

By design, Section 1634(a) "officially associates" Kaspersky Lab with a purported threat to national security, "creat[ing] a vilified class of one." *See Foretich*, 351 F.3d at 1224. This appears to have been the desired effect—to cause reputational damage that extends well beyond the federal government. In fact, in her September 4, 2017 *New York Times* op-ed, Senator Shaheen wrote: "Why then are federal agencies, local and state governments, and millions of Americans unwittingly inviting this threat [Kaspersky Lab] into their cyber networks and secure spaces?" J.A. 156.

As in *Foretich*, "it is the [statute's] specificity that renders the asserted nonpunitive purposes suspect. And, it is the [statute's] specificity that creates the injury to [Kaspersky Lab's] reputation." 351 F.3d at 1224. Therefore, "there exists a significant imbalance between the magnitude of the burden imposed and [the] purported nonpunitive purpose, [so] the statute cannot reasonably be said to further nonpunitive purposes." *Id*. at 1221–22 (citing *Consol. Edison*, 292 F.3d at 354);

see also id. at 1224 ("[T]he fact that Dr. Foretich was singled out for this severe burden belies the claim that Congress's purposes were nonpunitive. . . . It is the relative imbalance between the burden in this case and the implausible nonpunitive purposes that compels us toward a finding of punitiveness.").

d. The District Court should have considered less-burdensome alternatives.

When "an imbalance belies any purported nonpunitive goals, the availability of less burdensome alternatives becomes relevant to the bill of attainder analysis." *Foretich*, 351 F.3d at 1222 (internal quotation marks omitted) (citing *Nixon v. Adm'r of Gen. Servs.*, 433 U.S. 425, 482 (1977)). "[T]he availability of less burdensome alternatives can . . . cast doubt on purported nonpunitive purposes." *Id.* (citations omitted).

The Federal Acquisition Regulations ("FAR") establish a procedure for the federal government to debar contractors, and Congress could have referred the matter to the executive branch to consider such a proceeding. Congress could have made an effort to tailor the ban to the perceived threat, much as it might have enacted a law of general applicability. It did neither.

Section 1634(a)'s nonpunitive aims are not "sufficiently clear and convincing." *See Foretich*, 351 F.3d at 1221. "No wholly non-punitive purpose [can] justify" Section 1634(a)'s permanent, unconditional, and broad ban against all Kaspersky Lab hardware, software, and services. *See Consol. Edison*, 292 F.3d

at 351. The functional test demonstrates that Section 1634(a) is an unconstitutional bill of attainder.

3. The District Court misapplied the motivational test, because the legislative record evinces a congressional intent to punish.

Having failed to consider the appropriate contours of the historical and functional tests, as well as the proper application of those tests, the District Court compounded its errors when analyzing Section 1634(a) of the NDAA under the motivational test. "Evidence in the legislative history can bolster [a] conclusion [of punitiveness] . . . where other factors suggest punitiveness." *Foretich*, 351 F.3d at 1225. "[T]he Supreme Court has made clear that 'a formal legislative announcement of moral blameworthiness or punishment' is not necessary to an unlawful bill of attainder." *Id.* at 1226 (quoting *Nixon*, 433 U.S. at 480). "All that is necessary is that the legislative process and the law it produces indicate a congressional purpose to behave like a court and to censure or condemn." *Id.* (citing *United States v. Brown*, 381 U.S. 437, 453–54 (1965)).

There is no "formal" announcement in Section 1634(a) that Kaspersky Lab is blameworthy or disloyal, perhaps by design. As noted above, however, such an announcement is not required. There is compelling evidence that the legislative process that produced Section 1634(a), as well as the text itself, indicates a congressional purpose to censure or condemn Kaspersky Lab. "[T]he remarks of a

single legislator, even the sponsor, are not controlling in analyzing legislative history." *Chrysler Corp. v. Brown*, 441 U.S. 281, 311 (1979). But when the remarks of a sponsor "are consistent with the statutory language and other legislative history, they provide evidence of Congress' intent." *See Brock v. Pierce County*, 476 U.S. 253, 263 (1986) (citing *Grove City Coll. v. Bell*, 465 U.S. 555, 567 (1984)).[15]

Here, public statements by Senator Shaheen—who sponsored the amendment to the NDAA that singles out Kaspersky Lab—demonstrate the law's effect of punishing the company and branding it as disloyal to the United States. For example, Senator Shaheen penned a September 4, 2017 *New York Times* editorial about Kaspersky Lab that she titled: "The Russian Company That Is a Danger to Our Security." J.A. 156. The Senator alleged in the editorial that Kaspersky Lab's products create an "alarming national security vulnerability," *id.*, and that "Kaspersky Lab, with an active presence in millions of computer systems in the United States, is capable of playing a powerful role in [] an assault [on critical American infrastructure]," *id.* at 158.

---

15. *See also N. Haven Bd. of Educ. v. Bell*, 456 U.S. 512, 526–27 (1982) ("Senator Bayh's remarks, as those of the sponsor of the language ultimately enacted, are an authoritative guide to the statute's construction.").

Two weeks later, after her amendment was added to the NDAA by voice vote, Senator Shaheen issued a press release declaring that "[t]he case against Kaspersky Lab is overwhelming." *Id.* at 162. She added that "[t]he strong ties between Kaspersky Lab and the Kremlin are alarming and well-documented. . . . [M]y amendment . . . removes a real vulnerability to our national security." *Id.*[16]

There is nothing in the legislative history that contradicts the public statements on Section 1634(a) made by the legislator who sponsored the relevant statutory language. Those statements, although not part of the legislative history in the traditional sense, were widely distributed and are consistent with the plain text of the statute, which singles out Kaspersky Lab and no other specific entities. The District Court's observation that Congress could have punished Kaspersky Lab

16. Senator Shaheen's public remarks since the passage of the NDAA reiterate that her amendment is part of a larger effort to punish Kaspersky Lab. As recently as April 23, 2018, the Senator—referring to the NDAA—explained that she "led efforts in Congress to rid Kaspersky products from federal systems." *See* Joe Uchill, *US mulls sanctions against Kaspersky Lab*, Axios (Apr. 23, 2018), https://www.axios.com/us-mulls-sanctions-1524504874-62322aa5-06c3-4ea9-ad9b-a42c4cb8c035.html. She continued: "Sanctioning Kaspersky Lab is a logical next step." *Id.* If the Bill of Attainder Case had been allowed to proceed to discovery, Kaspersky Lab could have explored postenactment statements from Senator Shaheen, as well as other statements and evidence demonstrating Congress's intent to punish and the consequent harm to the company.

more harshly, *see id.* at 213 & n.13, is no support for the conclusion that Congress has not punished the company at all.

C. Kaspersky Lab stated a plausible claim that Section 1634(a) is a bill of attainder, and the District Court erred by granting the government's motion to dismiss.

This Court "reviews *de novo* the dismissal of a complaint for failure to state a claim, accepting a plaintiff's factual allegations as true and drawing all reasonable inferences in a plaintiff's favor." *Momenian v. Davidson*, 878 F.3d 381, 387 (D.C. Cir. 2017) (citing *Vila v. Inter-Am. Inv. Corp.*, 570 F.3d 274, 278 (D.C. Cir. 2009)). "To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). "Federal Rule of Civil Procedure 12(d) forbids considering facts beyond the complaint in connection with a motion to dismiss the complaint for failure to state a claim." *United States ex rel. Shea v. Cellco P'ship*, 863 F.3d 923, 936 (D.C. Cir. 2017).

1. The Bill of Attainder Complaint contains well-pleaded, non-speculative allegations showing that Kaspersky Lab is entitled to relief.

Rule 8(a) of the Federal Rules of Civil Procedure requires "a short and plain statement of the claim showing that the pleader is entitled to relief." The Rules "do not require 'detailed factual allegations' for a claim to survive a motion to

dismiss." *Banneker Ventures, L.L.C. v. Graham*, 798 F.3d 1119, 1129 (D.C. Cir. 2015) (quoting *Iqbal*, 556 U.S. at 678). "[A] well-pleaded complaint may proceed even if it strikes a savvy judge that actual proof of those facts is improbable, and 'that a recovery is very remote and unlikely.'" *Twombly*, 550 U.S. at 556 (quoting *Scheuer v. Rhodes*, 416 U.S. 232, 236 (1974)).

Kaspersky Lab alleged sufficient facts to support its constitutional claim and survive the government's motion to dismiss. *See* J.A. 142–50 ¶¶ 18–50. For example, Kaspersky Lab included with its complaint the enacted text, as well as prior versions, of the relevant provisions of Section 1634 of the NDAA that single out the company by name. *See id.* at 151–54, 159–60. Kaspersky Lab alleged that the targeted statute imposes impermissible legislative punishment by permanently banning Kaspersky Lab from doing business with the federal government, rendering the law an unconstitutional bill of attainder. *See id.* at 147–50 ¶¶ 38–44, 48–50.

In support, Kaspersky Lab cited in its complaint multiple public statements from the legislation's sponsor that constitute persuasive, and at least plausible, evidence that Congress's singling out of Kaspersky Lab was punishment intended to brand the company as untrustworthy or disloyal to the United States. *See id.* at 144–45 ¶ 28, 145 ¶ 31, 156–58, 162–63. Kaspersky Lab also alleged that Section 1634(a)'s permanent ban on providing any products or services to the federal

government, as well as the attendant stigma, "involve[s] profound reputational injuries" and "a substantial loss of sales." *Id.* at 149 ¶ 45. Because Kaspersky Lab has pled allegations that, if proved, would substantiate its constitutional challenge, its claim has "crosse[d] from conceivable to plausible." *See Banneker Ventures L.L.C.*, 798 F.3d at 1129.

2. The District Court erred by relying on evidence in the administrative record from the APA Case in granting a motion to dismiss under Rule 12(b)(6) in the Bill of Attainder Case.

Rather than credit Kaspersky Lab's well-pleaded allegations and reasonable inferences from them, the District Court weighed evidence from other sources and drew factual inferences *adverse* to Kaspersky Lab and in favor of the government to bolster its conclusion that Kaspersky Lab had not stated a plausible claim. In doing so, the District Court conflated the standards that apply to the separate underlying cases.

The procedural posture of the two cases is different. In the APA Case, Kaspersky Lab asserts that actions by an executive agency, the Department of Homeland Security, in issuing the BOD, were "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law" or "contrary to constitutional right, power, privilege, or immunity." *See* J.A. 21–22 ¶¶ 82–88 (quoting 5 U.S.C. § 706(2)(A) & (B)). Those questions are evaluated on the administrative record and, as a result, are typically decided on a motion or cross-motions for summary

judgment. The facts are not judicially noticed; the case is decided on the summary judgment standard limited to the administrative record. *See, e.g.*, *Leggett v. District of Columbia*, 793 F.3d 59, 66 (D.C. Cir. 2015); *Reid ex rel. Reid v. District of Columbia*, 401 F.3d 516, 522 (D.C. Cir. 2005). There is no basis for the District Court to rely on the administrative agency record in the APA Case to decide the government's motion to dismiss the constitutional challenge to congressional action presented in the Bill of Attainder Case. *See* Fed. R. Civ. P. 12(d).

The District Court summarized the rationale for Section 1634(a) of the NDAA as:

- Russia has committed cyberattacks;
- Kaspersky Lab cybersecurity products are present on federal government systems;
- all cybersecurity products can be used to exploit systems on which they are installed;
- Kaspersky Lab is headquartered in Russia, is subject to Russian laws, and "has certificates and licenses from the Federal Security Service" in Russia; and
- Eugene Kaspersky "graduated from an institute that was sponsored by the KGB," worked for the Ministry of Defense in the past, and has "personal ties with Russian intelligence officers."

See J.A. 173–82, 202–03 (citing, e.g., AR0106, AR0065, AR0557–58, AR0007, AR0011–13). The District Court reasoned that this "information" was "sufficient . . . to say that it was rational for Congress to conclude . . . that barring the federal

government's use of Kaspersky Lab products would help prevent further Russian cyber-attacks." *Id.* at 203. But this "information" does not appear in the Bill of Attainder Complaint or the NDAA legislative record; rather, it is drawn largely from the BOD administrative record, which Kaspersky Lab contests.[17] Furthermore, this congressional "conclusion" is a non sequitur based on little more than innuendo and suspicion.

The District Court further observed that Section 1634(a) is not punishment because it does not prevent Kaspersky Lab "from operating as a cybersecurity business." *Id.* at 197. "The company may still operate and derive revenue throughout the world, including in the United States, by selling its products to individuals, private companies, and other governments." *Id.*; *see id.* at 200 (Kaspersky Lab has been deprived of "one tiny source of revenue"); *id.* at 204 (The "burden" the NDAA imposes on Kaspersky Lab, "while real, is exaggerated by Plaintiffs."). These adverse factual inferences are contrary to the well-pleaded allegations of injury in the Complaint and cannot form the basis for resolving a motion to dismiss. *See Banneker Ventures, L.L.C.*, 798 F.3d at 1129 ("It is

17. On November 10, 2017, after the BOD took effect but before it became final, Kaspersky Lab filed a detailed written response that rebutted at length the legal arguments and factual allegations levied against Kaspersky Lab, corrected many misunderstandings, and highlighted the deficiencies in the administrative process. *See* J.A. 184.

inevitable that the defendant's [explanation] will sometimes prove to be the true one, but that does not relieve defendants of their obligation to respond to a complaint that states a plausible claim for relief, and to participate in discovery.").

3. The District Court erred by taking judicial notice of the truth of "all of the public records discussed" in its memorandum opinion.

The District Court's reliance on material from the APA Case was also erroneous because the court improperly took judicial notice of what it called "public records," including documents from the Department of Homeland Security's administrative record, in connection with evaluating a motion to dismiss in the Bill of Attainder Case. *See* J.A. 191 & n.5.

Rule 201 of the Federal Rules of Evidence "is the only evidence rule on the subject of judicial notice." Fed. R. Evid. 201 advisory committee's note to 1972 proposed rules. A court "may judicially notice a fact that is not subject to reasonable dispute because it: (1) is generally known within the trial court's territorial jurisdiction; or (2) can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned." Fed. R. Evid. 201(b). A party is entitled to be heard before a court takes judicial notice. *See* Fed. R. Evid. 201(e).

In *Hurd v. District of Columbia*, 864 F.3d 671 (D.C. Cir. 2017), this Court reversed a decision granting a motion to dismiss because the district court "looked

beyond the allegations of the complaint to evidence the [District of Columbia] government submitted." *Id.* at 686. This Court reasoned that the district court was not permitted to take judicial notice of the truth of the government's evidence at the motion-to-dismiss stage, even though the documents were part of the record in another case and the plaintiff did not dispute their authenticity. *See id.* ("[A]cquiescing to the authenticity of documents introduced in an earlier case is a far cry from agreeing that those documents present a full or fair picture of a matter a party has a right to dispute in a later case."). The Court offered an example: In "a defamation case, we drew on a filing in an unrelated case as a record of what was said. But we did not, and could not, rely on it for the truth of the matter asserted." *Id.* (citations omitted).

Here, as in *Hurd*, the District Court "relied on material beyond the pleadings to grant the motion to dismiss without permitting discovery and summary judgment briefing" in the Bill of Attainder Case. *See id.* at 686. For example, the court relied on various aspects of the administrative record from the APA Case in analyzing the bill of attainder claim. *See, e.g.*, J.A. 206 ("The record indicates that no other cybersecurity vendor had the same set of characteristics that had caused concerns about Kaspersky Lab. AR770. It was therefore reasonable for Congress to act only with respect to that company."); *id.* at 212 ("The purpose of BOD 17-01 in particular was to stem the risk of Russian cyber-attacks . . . . AR0629. It is

reasonable to assume that Congress had a similar motivation when . . . it passed a prohibition very similar to that BOD [Section 1634(a)] just days after [the BOD] was finalized.").

"In order to go beyond testing the adequacy of the allegations of the complaint, a district court must follow the procedures for converting a motion to dismiss into one for summary judgment." *Hurd*, 864 F.3d at 686–87. In particular, "district courts must provide the parties with notice and an opportunity to present evidence in support of their respective positions." *Kim v. United States*, 632 F.3d 713, 719 (D.C. Cir. 2011). It was error for the District Court to take judicial notice of material outside the Bill of Attainder Complaint and rely on that material for the truth of the matters asserted without converting the motion to dismiss into one for summary judgment and affording Kaspersky Lab the attendant procedural rights.

II. The District Court erred by dismissing for lack of standing Kaspersky Lab's substantive and procedural claims that the BOD is unlawful under the Administrative Procedure Act.

This Court reviews "a dismissal for lack of standing de novo." *Muir v. Navy Fed. Credit Union*, 529 F.3d 1100, 1105 (D.C. Cir. 2008) (citing *Info. Handling Servs., Inc. v. Def. Automated Printing Servs.*, 338 F.3d 1024, 1029 (D.C. Cir. 2003)). "To demonstrate standing, a plaintiff must show that she has suffered an 'injury in fact' that is 'fairly traceable' to the defendant's actions and that is 'likely to be redressed' by the relief she seeks." *Attias v. Carefirst, Inc.*, 865 F.3d 620,

625 (D.C. Cir. 2017) (quoting *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016)), *cert. denied*, 138 S. Ct. 981 (2018). A plaintiff demonstrates redressability "by showing 'that a favorable decision will relieve a discrete injury.'" *Energy Future Coal. v. EPA*, 793 F.3d 141, 144–45 (D.C. Cir. 2015) (quoting *Massachusetts v. EPA*, 549 U.S. 497, 525 (2007)). "The plaintiff 'need not show that a favorable decision will relieve' his or her '*every* injury.'" *Id.* at 145 (quoting *Massachusetts v. EPA*, 549 U.S. at 525).

As this Court has explained, "[e]ach element [of standing] must be supported in the same way as any other matter on which the plaintiff bears the burden of proof, *i.e.*, with the manner and degree of evidence required at the successive stages of the litigation." *Arpaio v. Obama*, 797 F.3d 11, 19 (D.C. Cir. 2015) (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561 (1992)). "[A]t the pleading stage, . . . plaintiffs are required only to 'state a *plausible* claim' that each of the standing elements is met." *Attias*, 865 F.3d at 625 (quoting *Food & Water Watch, Inc. v. Vilsack*, 808 F.3d 905, 913 (D.C. Cir. 2015)).[18]

---

18. The District Court dismissed the APA Case on the pleadings and not on summary judgment. *See* J.A. 173 ("Because the [APA Case] is dismissed for lack of standing, the Court need not reach the parties' cross-motions for summary judgment.").

In dismissing the APA Case on standing grounds, the District Court committed at least two errors. First, it assumed the correctness of its flawed analysis in the Bill of Attainder Case and reasoned that successful challenge of the BOD alone could not provide Kaspersky Lab any redress on its substantive APA claim. *See* J.A. 215–16 ("Regardless of the outcome of the [APA Case], those provisions of the NDAA will be the law. Sections 1634(a) and (b) of that law cause, *at least*, the same alleged harms as BOD 17-01.").[19] Second, the court declined to apply the correct standard for determining whether a litigant has adequately alleged redress for a procedural harm.

A. Kaspersky Lab plausibly alleged a discrete injury caused by the BOD that is redressable by a favorable court decision.

The District Court, having dismissed the Bill of Attainder Complaint, concluded that Section 1634(a) of the NDAA would bar any relief Kaspersky Lab might receive if the court invalidated the BOD, so the APA claim was not redressable. Because the dismissal of the Bill of Attainder Complaint was legally incorrect and procedurally improper, it necessarily follows that the dismissal of the

19. The District Court also suggested that Kaspersky Lab was required to challenge the BOD and the NDAA in a single lawsuit to demonstrate redressability, *see id.* at 216, even though the court consolidated the cases for briefing and decided them in the same memorandum opinion.

APA Case was erroneous as well. Furthermore, Kaspersky Lab plausibly alleged a discrete injury caused by the BOD that is redressable by a favorable court decision.

The issuance of the BOD on September 13, 2017, before passage of the NDAA and without prior opportunity for public notice or comment, triggered immediate steps by federal agencies to identify and remove Kaspersky Lab-branded products from federal systems. *See* J.A. 3–4 ¶¶ 6–10. "The BOD . . . effectively banned all U.S. government agencies from using Kaspersky products and debarred the company immediately." *Id.* at 8 ¶ 35. As Kaspersky Lab explained, it "has a substantial interest in its status as a vendor to the U.S. Government, and in its continued ability to sell its product[s] to the U.S. Government." *Id.* at 8 ¶ 34. That ability, at least with respect to products covered by the BOD, was extinguished upon the BOD's issuance.

The adverse reputational effects were also immediate. In the decision accompanying the BOD, the Department of Homeland Security "branded Kaspersky Lab products a threat to U.S. national security." *See id.* at 8–9 ¶ 35. Christopher Krebs, the Senior Official Performing the Duties of the Under Secretary for the National Protection and Programs Directorate, stated in a response to a question about consumer reaction to the BOD: "[W]hen [the Department of Homeland Security] makes a pretty bold statement like issuing the Kaspersky Lab binding operational directive I think that's a fairly strong signal [to

consumers]." *Id.* at 13 ¶ 51 (citing *Is the US Losing the Cyber Battle?*, Aspen Institute (Oct. 31, 2017), https://www.aspeninstitute.org/events/us-losing-cyber-battle/).

The District Court erred by not recognizing that invalidation of the BOD would redress a discrete injury to Kaspersky Lab, even if it did not redress "*every* injury." *See Energy Future Coal.*, 793 F.3d at 145 (quoting *Massachusetts v. EPA*, 549 U.S. at 525). Invalidating the BOD may not cure all the economic and reputational injuries caused by the federal government's mistreatment of Kaspersky Lab, but it could "constitute a 'necessary first step on a path that could ultimately lead to relief fully redressing the injury.'" *See Tel. & Data Sys., Inc. v. FCC*, 19 F.3d 42, 47 (D.C. Cir. 1994) (quoting *Hazardous Waste Treatment Council v. EPA*, 861 F.2d 270, 273 (D.C. Cir. 1988)). For example, Kaspersky Lab's ability to fully redress the severe reputational damage caused by the federal government requires, at least, successful challenges to both the BOD *and* the NDAA. A decision that the Department of Homeland Security's BOD is unlawful would in fact "produce tangible, meaningful results in the real world." *See Tel. & Data Sys., Inc.*, 19 F.3d at 47 (citation omitted).

B. Kaspersky Lab was not required to prove that proper procedural due process would have produced a different substantive result.

Where a plaintiff "alleges a deprivation of a procedural protection to which he is entitled[,] [he] never has to prove that if he had received the procedure the substantive result would have been altered." *NB ex rel. Peacock v. District of Columbia*, 682 F.3d 77, 86 (D.C. Cir. 2012) (quoting *Sugar Cane Growers Coop. of Fla. v. Veneman*, 289 F.3d 89, 94 (D.C. Cir. 2002)). This Court applies "this relaxed standard for redressability in procedural rights cases." *Id.* (internal quotation marks and alterations omitted).

Here, Kaspersky Lab framed its APA Case as alleging not only a deprivation of a protected substantive right, but also deprivation "with constitutionally insufficient procedures attendant upon that deprivation." J.A. 21 ¶ 85. The Department of Homeland Security failed to provide Kaspersky Lab notice or a meaningful opportunity to be heard *before* the agency issued the BOD on September 13, 2017. *See id.* at 8–9 ¶ 35, 12–15 ¶¶ 48–58. And its postdeprivation invitation for comment on the BOD was deficient. *See id.* at 11–12 ¶ 47, 15–16 ¶¶ 59–61. Kaspersky Lab is not required to show that the Department of Homeland Security would not have issued the BOD—or that the BOD would have been significantly different in substance—to establish standing for its procedural

due process claim. The District Court erred by ignoring Kaspersky Lab's procedural claim.

Conclusion

For the foregoing reasons, the orders of the District Court should be reversed.

Dated: June 27, 2018

Respectfully submitted,

/s/ Ryan P. Fayhee

Ryan P. Fayhee, D.C. Bar No. 1033852
Scott H. Christensen, D.C. Bar No. 476439
Stephen R. Halpin III, D.C. Bar No. 1048974
HUGHES HUBBARD & REED LLP
1775 I Street, N.W., Suite 600
Washington, D.C. 20006-2401
Telephone: (202) 721-4600
Facsimile: (202) 721-4646
Email: ryan.fayhee@hugheshubbard.com
Email: scott.christensen@hugheshubbard.com
Email: stephen.halpin@hugheshubbard.com

Attorneys for Plaintiffs–Appellants Kaspersky Lab, Inc. and Kaspersky Labs Limited

CERTIFICATE OF COMPLIANCE

I certify that, pursuant to Fed. R. App. P. 32 (a)(7)(B), the foregoing Brief of Appellants is proportionately spaced, has a typeface of 14-point or more, and contains 12,281 words excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

Dated: June 27, 2018

/s/ Ryan P. Fayhee

Ryan P. Fayhee
HUGHES HUBBARD & REED LLP
1775 I Street, N.W.
Washington, D.C. 20006-2401
Telephone: (202) 721-4600
Email: ryan.fayhee@hugheshubbard.com

Attorney for Plaintiffs–Appellants

CERTIFICATE OF SERVICE

I hereby certify that on June 27, 2018, I electronically filed the foregoing Brief of Appellants, as well as the Joint Appendix, with the Clerk of the Court for the United States Court of Appeals for the District of Columbia Circuit by using the appellate CM/ECF system. Participants in the case who are registered CM/ECF users will be served by the appellate CM/ECF system. I also hereby certify that I have caused copies of the foregoing Brief of Appellants, as well as the Joint Appendix, to be filed by hand with the Clerk and to be served on the following:

H. Thomas Byron III
Assistant Director
Lewis S. Yelin
Senior Counsel
Civil Division, Appellate Staff
U.S. Department of Justice
Main (RFK) Room 7529
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530
Office: (202) 616-5367
Fax: (202) 307-2551
H.Thomas.Byron@usdoj.gov
Lewis.Yelin@usdoj.gov

Sam M. Singer
Trial Attorney
Civil Division, Federal Programs Branch
U.S. Department of Justice
Office: (202) 616-8014
Fax: (202) 616-8460
Samuel.M.Singer@usdoj.gov

Dated: June 27, 2018

/s/ Ryan P. Fayhee
Ryan P. Fayhee D.C. Bar No. 1033852

ADDENDUM

Table of Contents

Page

One Hundred Fifteenth Congress of the United States of America

AT THE FIRST SESSION

Begun and held at the City of Washington on Tuesday, the third day of January, two thousand and seventeen

An Act

To authorize appropriations for fiscal year 2018 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

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

SECTION 1. SHORT TITLE.

This Act may be cited as the "National Defense Authorization Act for Fiscal Year 2018".

SEC. 2. ORGANIZATION OF ACT INTO DIVISIONS; TABLE OF CONTENTS.

(a) DIVISIONS.—This Act is organized into four divisions as follows:

(1) Division A—Department of Defense Authorizations.

(2) Division B—Military Construction Authorizations.

(3) Division C—Department of Energy National Security Authorizations and Other Authorizations.

(4) Division D—Funding Tables.

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

cyber activities that are carried out against infrastructure critical to the political integrity, economic security, and national security of the United States.

(4) Available or planned cyber capabilities that may be used to impose costs on any foreign power targeting the United States or United States persons with a cyber attack or malicious cyber activity.

(5) Development of multi-prong response options, such as—

(A) boosting the cyber resilience of critical United States strike systems (including cyber, nuclear, and non-nuclear systems) in order to ensure the United States can credibly threaten to impose unacceptable costs in response to even the most sophisticated large-scale cyber attack;

(B) developing offensive cyber capabilities and specific plans and strategies to put at risk targets most valued by adversaries of the United States and their key decision makers; and

(C) enhancing attribution capabilities and developing intelligence and offensive cyber capabilities to detect, disrupt, and potentially expose malicious cyber activities.

(c) LIMITATION ON AVAILABILITY OF FUNDS.—

(1) IN GENERAL.—Of the funds authorized to be appropriated by this Act or otherwise made available for fiscal year 2018 for procurement, research, development, test and evaluation, and operations and maintenance, for the covered activities of the Defense Information Systems Agency, not more than 60 percent may be obligated or expended until the date on which the President submits to the appropriate congressional committees the report under subsection (a)(2).

(2) COVERED ACTIVITIES DESCRIBED.—The covered activities referred to in paragraph (1) are the activities of the Defense Information Systems Agency in support of—

(A) the White House Communication Agency; and

(B) the White House Situation Support Staff.

(d) DEFINITIONS.—In this section:

(1) The term "foreign power" has the meaning given that term in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(2) The term "appropriate congressional committees" means—

(A) the congressional defense committees;

(B) the Committee on Foreign Affairs, the Committee on Homeland Security, and the Committee on the Judiciary of the House of Representatives; and

(C) the Committee on Foreign Relations, the Committee on Homeland Security and Governmental Affairs, and the Committee on the Judiciary of the Senate.

SEC. 1634. PROHIBITION ON USE OF PRODUCTS AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB.

(a) PROHIBITION.—No department, agency, organization, or other element of the Federal Government may use, whether directly or through work with or on behalf of another department, agency, organization, or element of the Federal Government, any hardware, software, or services developed or provided, in whole or in part, by—

(1) Kaspersky Lab (or any successor entity);

(2) any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or

(3) any entity of which Kaspersky Lab has majority ownership.

(b) EFFECTIVE DATE.—The prohibition in subsection (a) shall take effect on October 1, 2018.

(c) REVIEW AND REPORT.—

(1) REVIEW.—The Secretary of Defense, in consultation with the Secretary of Energy, the Secretary of Homeland Security, the Attorney General, the Administrator of the General Services Administration, and the Director of National Intelligence, shall conduct a review of the procedures for removing suspect products or services from the information technology networks of the Federal Government.

(2) REPORT.—

(A) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, Secretary of Defense shall submit to the appropriate congressional committees a report on the review conducted under paragraph (1).

(B) ELEMENTS.—The report under subparagraph (A) shall include the following:

(i) A description of the Federal Government-wide authorities that may be used to prohibit, exclude, or prevent the use of suspect products or services on the information technology networks of the Federal Government, including—

(I) the discretionary authorities of agencies to prohibit, exclude, or prevent the use of such products or services;

(II) the authorities of a suspension and debarment official to prohibit, exclude, or prevent the use of such products or services;

(III) authorities relating to supply chain risk management;

(IV) authorities that provide for the continuous monitoring of information technology networks to identify suspect products or services; and

(V) the authorities provided under the Federal Information Security Management Act of 2002.

(ii) Assessment of any gaps in the authorities described in clause (i), including any gaps in the enforcement of decisions made under such authorities.

(iii) An explanation of the capabilities and methodologies used to periodically assess and monitor the information technology networks of the Federal Government for prohibited products or services.

(iv) An assessment of the ability of the Federal Government to periodically conduct training and exercises in the use of the authorities described in clause (i)—

(I) to identify recommendations for streamlining process; and

(II) to identify recommendations for education and training curricula, to be integrated into existing training or certification courses.

(v) A description of information sharing mechanisms that may be used to share information about suspect products or services, including mechanisms for the sharing of such information among the Federal Government, industry, the public, and international partners.

(vi) Identification of existing tools for business intelligence, application management, and commerce due-diligence that are either in use by elements of the Federal Government, or that are available commercially.

(vii) Recommendations for improving the authorities, processes, resourcing, and capabilities of the Federal Government for the purpose of improving the procedures for identifying and removing prohibited products or services from the information technology networks of the Federal Government.

(viii) Any other matters the Secretary determines to be appropriate.

(C) FORM.—The report under subparagraph (A) shall be submitted in unclassified form, but may include a classified annex.

(3) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this section, the term "appropriate congressional committees" means the following:

(A) The Committee on Armed Services, the Committee on Energy and Commerce, the Committee on Homeland Security, the Committee on the Judiciary, the Committee on Oversight and Government Reform, and the Permanent Select Committee on Intelligence of the House of Representatives.

(B) The Committee on Armed Services, the Committee on Energy and Natural Resources, the Committee on Homeland Security and Governmental Affairs, the Committee on the Judiciary, and the Select Committee on Intelligence of the Senate.

SEC. 1635. MODIFICATION OF AUTHORITIES RELATING TO ESTABLISHMENT OF UNIFIED COMBATANT COMMAND FOR CYBER OPERATIONS.

Section 167b of title 10, United States Code, is amended—

(1) by striking subsection (d); and

(2) by redesignating subsections (e) and (f) as subsections (d) and (e), respectively.

SEC. 1636. MODIFICATION OF DEFINITION OF ACQUISITION WORKFORCE TO INCLUDE PERSONNEL CONTRIBUTING TO CYBERSECURITY SYSTEMS.

Section 1705(h)(2)(A) of title 10, United States Code, is amended—

(1) by inserting "(i)" after "(A)";

(2) by striking "; and" and inserting "; or"; and

(3) by adding at the end the following new clause:

"(ii) contribute significantly to the acquisition or development of systems relating to cybersecurity; and".

Dated: September 11, 2017.

Ira S. Reese,

Executive Director, Laboratories and Scientific Services Directorate.

[FR Doc. 2017–19863 Filed 9–18–17; 8:45 am]

BILLING CODE 9111–14–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

Waiver of Compliance With Navigation Laws; Hurricanes Harvey and Irma

AGENCY: Office of the Secretary, Department of Homeland Security.

ACTION: Notice.

On September 8, 2017, I issued a limited waiver of the Jones Act upon the recommendation of the Department of Energy and at the request of the Department of Defense.[1] Hurricane Harvey striking the U.S. Gulf Coast has resulted in severe disruptions in both the midstream and downstream sectors of the oil supply system. Some refineries and pipeline networks are shut-in or running at reduced rates. Thus, conditions exist for a continued shortage of energy supply in areas predicted to be affected by Hurricane Irma. In light of this, the Department of Energy has recommended that the Department of Homeland Security waive the requirements of the Jones Act in the interest of national defense to facilitate the transportation of the necessary volume of petroleum products through September 22, 2017. Furthermore, the Department of Defense has requested a waiver of the Jones Act in the interest of national defense through September 22, 2017, commencing immediately.

The Jones Act, 46 United States Code (U.S.C.) 55102, states that a vessel may not provide any part of the transportation of merchandise by water, or by land and water, between points in the United States to which the coastwise laws apply, either directly or via a foreign port unless the vessel was built in and documented under the laws of the United States and is wholly owned by persons who are citizens of the United States. Such a vessel, after obtaining a coastwise endorsement from the U.S. Coast Guard, is ''coastwise-qualified.'' The coastwise laws generally apply to points in the territorial sea, which is defined as the belt, three nautical miles wide, seaward of the territorial sea baseline, and to points located in internal waters, landward of the territorial sea baseline.

The navigation laws, including the coastwise laws, can be waived under the authority provided by 46 U.S.C. 501. The statute provides in relevant part that on request of the Secretary of Defense, the head of an agency responsible for the administration of the navigation or vessel-inspection laws shall waive compliance with those laws to the extent the Secretary considers necessary in the interest of national defense. 46 U.S.C. 501(a).

For the reasons stated above, and in light of the request from the Department of Defense and the concurrence of the Department of Energy, I am exercising my authority to waive the Jones Act through September 22, 2017, commencing immediately, to facilitate movement of refined petroleum products, including gasoline, diesel, and jet fuel, to be shipped from New York, New Jersey, Delaware, Maryland, Pennsylvania, New Mexico, Texas, Louisiana, Mississippi, Alabama, and Arkansas to Florida, Georgia, South Carolina, North Carolina, Virginia, West Virginia, and Puerto Rico. This waiver applies to covered merchandise laded on board a vessel through and including September 22, 2017.

Executed this 12th day of September, 2017.

Elaine C. Duke,

Acting Secretary of Homeland Security.

[FR Doc. 2017–19902 Filed 9–18–17; 8:45 am]

BILLING CODE 9111–14–P

DEPARTMENT OF HOMELAND SECURITY

National Protection and Programs Directorate; Notification of Issuance of Binding Operational Directive 17–01 and Establishment of Procedures for Responses

AGENCY: National Protection and Programs Directorate, DHS.

ACTION: Issuance of binding operational directive; procedures for responses; notice of availability.

SUMMARY: In order to safeguard Federal information and information systems, DHS has issued a binding operational directive to all Federal, executive branch departments and agencies relating to information security products, solutions, and services supplied, directly or indirectly, by AO Kaspersky Lab or affiliated companies. The binding operational directive requires agencies to identify Kaspersky-branded products (as defined in the directive) on Federal information systems, provide plans to discontinue use of Kaspersky-branded products, and, at 90 calendar days after issuance of the directive, unless directed otherwise by DHS in light of new information, begin to remove Kaspersky-branded products. DHS is also establishing procedures, which are detailed in this notice, to give entities whose commercial interests are directly impacted by this binding operational directive the opportunity to respond, provide additional information, and initiate a review by DHS.

DATES: Binding Operational Directive 17–01 was issued on September 13, 2017. DHS must receive responses from impacted entities on or before November 3, 2017.

ADDRESSES: Submit electronic responses to Binding Operational Directive 17–01, along with any additional information or evidence, to *BOD.Feedback@hq.dhs.gov.*

SUPPLEMENTARY INFORMATION: The Department of Homeland Security (''DHS'' or ''the Department'') has the statutory responsibility, in consultation with the Office of Management and Budget, to administer the implementation of agency information security policies and practices for information systems, which includes assisting agencies and providing certain government-wide protections. 44 U.S.C. 3553(b). As part of that responsibility, the Department is authorized to ''develop[ ] and oversee[ ] the implementation of binding operational directives to agencies to implement the policies, principles, standards, and guidance developed by the Director [of the Office of Management and Budget] and [certain] requirements of [the Federal Information Security Modernization Act of 2014.]'' 44 U.S.C. 3553(b)(2). A binding operational directive (''BOD'') is ''a compulsory direction to an agency that (A) is for purposes of safeguarding Federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk; [and] (B) [is] in accordance with policies, principles, standards, and guidelines issued by the Director[.]'' 44 U.S.C. 3552(b)(1). Agencies are required to comply with these directives. 44 U.S.C. 3554(a)(1)(B)(ii).

Overview of BOD 17–01

In carrying out this statutory responsibility, the Department issued BOD 17–01, titled ''Removal of Kaspersky-Branded Products.'' The text of BOD 17–01 is reproduced in the next section of this document.

[1] Published in the **Federal Register** at 82 FR 43248 (Sept. 14, 2017).

Binding Operational Directive 17–01 may have adverse consequences for the commercial interests of AO Kaspersky Lab or other entities. Therefore, the Department will provide entities whose commercial interests are directly impacted by BOD 17–01 the opportunity to respond to the BOD, as detailed in the Administrative Process for Responding to Binding Operational Directive 17–01 section of this notice, below.

Text of BOD 17–01

Binding Operational Directive BOD–17–01
Original Issuance Date: September 13, 2017
Applies to: All Federal Executive Branch Departments and Agencies
FROM: Elaine C. Duke, Acting Secretary, Department of Homeland Security
CC: Mick Mulvaney, Director, Office of Management and Budget
SUBJECT: Removal of Kaspersky-Branded Products

A binding operational directive is a compulsory direction to Federal, executive branch, departments and agencies for purposes of safeguarding Federal information and information systems. 44 U.S.C. 3552(b)(1). The Department of Homeland Security (DHS) develops and oversees the implementation of binding operational directives pursuant to the Federal Information Security Modernization Act of 2014 (''FISMA''). 44 U.S.C. 3553(b)(2). Federal agencies are required to comply with these DHS-developed directives. 44 U.S.C. 3554(a)(1)(B)(ii). DHS binding operational directives do not apply to statutorily defined ''National Security Systems'' nor to certain systems operated by the Department of Defense and the Intelligence Community. 44 U.S.C. 3553(d)–(e).

Background: DHS, in consultation with interagency partners, has determined that the risks presented by Kaspersky-branded products justify issuance of this Binding Operational Directive.

Definitions:

• ''Agencies'' means all Federal, executive branch, departments and agencies. This directive does not apply to statutorily defined ''National Security Systems'' nor to certain systems operated by the Department of Defense and the Intelligence Community. 44 U.S.C. 3553(d)–(e)

• ''Kaspersky-branded products'' means information security products, solutions, and services supplied, directly or indirectly, by AO Kaspersky Lab or any of its predecessors, successors, parents, subsidiaries, or affiliates, including Kaspersky Lab North America, Kaspersky Lab, Inc., and Kaspersky Government Security Solutions, Inc. (collectively, ''Kaspersky''), including those identified below.

Kaspersky-branded products currently known to DHS are: Kaspersky Anti-Virus; Kaspersky Internet Security; Kaspersky Total Security; Kaspersky Small Office Security; Kaspersky Anti Targeted Attack; Kaspersky Endpoint Security; Kaspersky Cloud Security (Enterprise); Kaspersky Cybersecurity Services; Kaspersky Private Security Network; and Kaspersky Embedded Systems Security.

This directive does not address Kaspersky code embedded in the products of other companies. It also does not address the following Kaspersky services: Kaspersky Threat Intelligence and Kaspersky Security Training.

• ''Federal information system'' means an information system used or operated by an agency or by a contractor of an agency or by another organization on behalf of an agency.

Required Actions: All agencies are required to:

1. Within 30 calendar days after issuance of this directive, identify the use or presence of Kaspersky-branded products on all Federal information systems and provide to DHS a report that includes:

a. A list of Kaspersky-branded products found on agency information systems. If agencies do not find the use or presence of Kaspersky-branded products on their Federal information systems, inform DHS that no Kaspersky-branded products were found.

b. The number of endpoints impacts by each product, and

c. The methodologies employed to identify the use or presence of the products.

2. Within 60 calendar days after issuance of this directive, develop and provide to DHS a detailed plan of action to remove and discontinue present and future use of all Kaspersky-branded products beginning 90 calendar days after issuance of this directive. Agency plans must address the following elements in the attached template [1] at a minimum:

a. Agency name.

b. Point of contact information, including name, telephone number, and email address.

c. List of identified products.

d. Number of endpoints impacted.

e. Methodologies employed to identify the use or presence of the products.

f. List of Agencies (components) impacted within Department.

g. Mission function of impacted endpoints and/or systems.

h. All contracts, service-level agreements, or other agreements your agency has entered into with Kaspersky.

i. Timeline to remove identified products.

j. If applicable, FISMA performance requirements or security controls that product removal would impact, including but not limited to data loss/leakage prevention, network access control, mobile device management, sandboxing/detonation chamber, Web site reputation filtering/web content filtering, hardware and software whitelisting, vulnerability and patch management, anti-malware, anti-exploit, spam filtering, data encryption, or other capabilities.

k. If applicable, chosen or proposed replacement products/capabilities.

l. If applicable, timeline for implementing replacement products/capabilities.

m. Foreseeable challenges not otherwise addressed in this plan.

n. Associated costs related to licenses, maintenance, and replacement (please coordinate with agency Chief Financial Officers).

3. At 90 calendar days after issuance of this directive, and unless directed otherwise by DHS based on new information, begin to implement the agency plan of action and provide a status report to DHS on the progress of that implementation every 30 calendar days thereafter until full removal and discontinuance of use is achieved.

DHS Actions:

• DHS will rely on agency self-reporting and independent validation measures for tracking and verifying progress.

• DHS will provide additional guidance through the Federal Cybersecurity Coordination, Assessment, and Response Protocol (the C–CAR Protocol) following the issuance of this directive.

Potential Budgetary Implications: DHS understands that compliance with this BOD could result in budgetary implications. Agency Chief Information Officers (CIOs) and procurement officers should coordinate with the agency Chief Financial Officer (CFO), as appropriate.

DHS Point of Contact: Binding Operational Directive Team.[2]

[1] The template for agency plans has not been reproduced in the **Federal Register**, but is available (in electronic format) from DHS upon request.

[2] The email address to be used by Federal agencies to contact the DHS Binding Operational

Continued

Attachment: BOD 17–01 Plan of Action Template.[3]

Administrative Process for Responding to Binding Operational Directive 17–01

The Department will provide entities whose commercial interests are directly impacted by BOD 17–01 the opportunity to respond to the BOD, as detailed below:

- The Department has notified Kaspersky about BOD 17–01 and outlined the Department's concerns that led to the decision to issue this BOD. This correspondence with Kaspersky is available (in electronic format) to other parties whose commercial interests are directly impacted by BOD–17–01, upon request. Requests must be directed to *BOD.Feedback@hq.dhs.gov.*
- If it wishes to initiate a review by DHS, by November 3, 2017, Kaspersky, and any other entity that claims its commercial interests will be directly impacted by the BOD, must provide the Department with a written response and any additional information or evidence supporting the response, to explain the adverse consequences, address the Department's concerns, or mitigate those concerns.
- The Department's Assistant Secretary for Cybersecurity and Communications, or another official designated by the Secretary of Homeland Security (''the Secretary''), will review the materials relevant to the issues raised by the entity, and will issue a recommendation to the Secretary regarding the matter. The Secretary's decision will be communicated to the entity in writing by December 13, 2017.
- The Secretary reserves the right to extend the timelines identified above.

Elaine C. Duke,

Secretary of Homeland Security (Acting), Department of Homeland Security.

[FR Doc. 2017–19838 Filed 9–18–17; 8:45 am]

BILLING CODE 9910–9P–P

DEPARTMENT OF THE INTERIOR

Bureau of Indian Affairs

[178A2100DD/AAKC001030/ A0A501010.999900 253G]

Proclaiming Certain Lands as Reservation for the Jamestown S'Klallam Tribe of Washington

AGENCY: Bureau of Indian Affairs, Interior.

ACTION: Notice of reservation proclamation.

SUMMARY: This notice informs the public that the Acting Assistant Secretary—Indian Affairs proclaimed approximately 267.29 acres, more or less, an addition to the reservation of the Jamestown S'Klallam Tribe on July 21, 2017.

FOR FURTHER INFORMATION CONTACT: Ms. Sharlene M. Round Face, Bureau of Indian Affairs, Division of Real Estate Services, 1849 C Street NW., MS–4642–MIB, Washington, DC 20240, Telephone: (202) 208–3615.

SUPPLEMENTARY INFORMATION: This notice is published in the exercise of authority delegated by the Secretary of the Interior to the Assistant Secretary—Indian Affairs by part 209 of the Departmental Manual.

A proclamation was issued according to the Act of June 18, 1934 (48 Stat. 986; 25 U.S.C. 5110) for the land described below. The land was proclaimed to be the Jamestown S'Klallam Reservation for the Jamestown S'Klallam Tribe, Clallam County, State of Washington.

Jamestown S'Klallam Reservation for the Jamestown S'Klallam Tribe

14 Parcels—Legal Description Containing 267.29 Acres, More or Less

Tribal Tract Number: 129–T1004

Legal description containing 5.090 acres, more or less.

That portion of Lot 28 of Keeler's Sunrise Beach, as recorded in Volume 4 of plats, page 46, records of Clallam County, Washington, lying between the Northeasterly right of way line of the Chicago, Milwaukee, St. Paul and Pacific Railway and the Northeasterly right of way line of the present existing State Highway No. 9 and bounded on the Southeasterly end by the Northerly right of way line of the existing Old Olympic Highway;

Also, that portion of the Northeast Quarter of the Southeast Quarter of Section 34, Township 30 North, Range 3 West, W.M., Clallam County, Washington, lying between the Northeasterly right of way line of the Chicago, Milwaukee, St. Paul and Pacific Railway and the Northeasterly right of way line of the present existing State Highway No. 9.

Excepting therefrom that portion of the Northeast Quarter of the Southeast Quarter of said Section 34, Township 30 North, Range 3 West, W.M., Clallam County, Washington, described as follows starting and ending at the point identified as the *True Point Of Beginning:*

Commencing at the East Quarter Corner of said Section 34; thence North 87°42′55″ West, a distance of 317.69 feet along the North Line of the said Northeast Quarter of the Southeast Quarter to a point lying on the Northeasterly right-of-way line of the abandoned Chicago, Milwaukee, St. Paul and Pacific Railroad and the *True Point Of Beginning;* Thence South 49°56′33″ East along said right-of-way line, a distance of 112.08 feet to a point lying on a tangent curve, concave Southwesterly and having a radius of 2914.62 feet; Thence Southeasterly along said curve through a central angle of 05°25′36″, an arc length of 276.05 feet; Thence leaving said curve North 85°53′09″ West, a distance of 33.08 feet; Thence North 46°13′33″ West, a distance of 372.52 feet to the North line of said Northeast Quarter of the Southeast Quarter; Thence South 87°42′55″ East along said North line, a distance of 13.65 feet to the *True Point of Beginning.* As described in Boundary Line Agreement recorded May 29, 2007 as Recording No. 2007–1201967. Said instrument is a re-recording of Auditor's File No. 2007–1200907 and 2007–1201792. Situate in the County of Clallam, State of Washington. Containing 5.090 acres, more or less.

Tribal Tract Number: 130–T1169

Legal description containing 30.36 acres, more or less.

Parcel A: The East Half of the Southeast Quarter of the Northeast Quarter and the Southeast Quarter of the Northeast Quarter of the Northeast Quarter in Section 11, Township 30 North, Range 4 West, W.M., Clallam County, Washington.

Parcel B: An easement for ingress, egress and utilities over a 30 foot easement along the East Line of the Northeast Quarter of the Northeast Quarter of the Northeast Quarter in Section 11, Township 30 North, Range 4 West, W.M., Clallam County, Washington. Containing 30.36 acres, more or less.

Tribal Tract Number: 129–T1003

Legal description containing 5.00 acres, more or less.

Parcel A: That portion of the South Half of the Northeast Quarter of the Northeast Quarter of Section 26, Township 30 North, Range 4 West, W.M., Clallam County, Washington, described as Parcel 1 as delineated on Survey recorded in Volume 4 of Surveys, page 25, under Auditor's File No. 497555, situate in Clallam County, State of Washington.

Parcel B: An easement for ingress, egress and utilities over, under and

Directive Team has not been reproduced in the **Federal Register**.

[3] The template for agency plans has not been reproduced in the **Federal Register,** but is available (in electronic format) from DHS upon request.

DEPARTMENT OF DEFENSE

GENERAL SERVICES ADMINISTRATION

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

48 CFR Parts 1, 4, 13, 39, and 52

[FAC 2005–99; FAR Case 2018–010; Item I; Docket 2018–0010, Sequence 1]

RIN 9000–AN64

Federal Acquisition Regulation; Use of Products and Services of Kaspersky Lab

AGENCY: Department of Defense (DoD), General Services Administration (GSA), and National Aeronautics and Space Administration (NASA).

ACTION: Interim rule.

SUMMARY: DoD, GSA, and NASA are issuing an interim rule amending the Federal Acquisition Regulation (FAR) to implement a section of the National Defense Authorization Act for Fiscal Year 2018.

DATES:

Effective Date: July 16, 2018.

Applicability Dates:

- Contracting officers shall include the clause at FAR 52.204–23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab or Other Covered Entities—
- In solicitations issued on or after July 16, 2018, and resultant contracts; and
- In solicitations issued before July 16, 2018, provided award of the resulting contract(s) occurs on or after July 16, 2018.
- Contracting officers shall modify, in accordance with FAR 1.108(d)(3), existing indefinite-delivery contracts to include the FAR clause for future orders, prior to placing any further orders on or after July 16, 2018.
- If modifying an existing contract to extend the period of performance by more than 6 months, contracting officers should include the clause in accordance with 1.108(d).

Comment Date: Interested parties should submit written comments to the Regulatory Secretariat on or before August 14, 2018 to be considered in the formulation of a final rule.

ADDRESSES: Submit comments identified by FAC 2005–99, FAR Case 2018–010, by any of the following methods:

- *Regulations.gov: http://www.regulations.gov.* Submit comments via the Federal eRulemaking portal by searching for ''FAR Case 2018–010''. Select the link ''Submit a Comment'' that corresponds with ''FAR Case 2018–010.'' Follow the instructions provided at the ''Submit a Comment'' screen. Please include your name, company name (if any), and ''FAR Case 2018–010'' on your attached document.
- *Mail:* General Services Administration, Regulatory Secretariat (MVCB), ATTN: Lois Mandell, 1800 F Street NW, 2nd Floor, Washington, DC 20405–0001.

Instructions: Please submit comments only and cite FAC 2005–99, FAR Case 2018–010, in all correspondence related to this case. All comments received will be posted without change to *http://www.regulations.gov,* including any personal and/or business confidential information provided.

FOR FURTHER INFORMATION CONTACT: Ms. Camara Francis, Procurement Analyst, at 202–550–0935, for clarification of content. For information pertaining to status or publication schedules, contact the Regulatory Secretariat at 202–501–4755. Please cite FAC 2005–99, FAR Case 2018–010.

SUPPLEMENTARY INFORMATION:

I. Background

This interim rule revises the FAR to implement section 1634 of Division A of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2018 (Pub. L. 115–91). Section 1634 of this law prohibits the use of hardware, software, and services of Kaspersky Lab and its related entities by the Federal Government on or after October 1, 2018.

Implementation of this rule in the FAR should not impact or impair any other planned or ongoing efforts agencies may undertake to implement section 1634 of Division A of the NDAA for FY 2018, including consideration by agencies of the presence of hardware, software, or services developed or provided by Kaspersky Lab as a technical evaluation factor in the source selection process.

II. Discussion and Analysis

This rule amends FAR part 4, adding a new subpart 4.20, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab, with a corresponding new contract clause at 52.204–23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities. The rule also adds text in subpart 13.2, Actions at or Below the Micro-Purchase Threshold, to address section 1634 with regard to micro-purchases.

To implement section 1634, the clause at 52.204–23 prohibits contractors from providing any hardware, software, or services developed or provided by Kaspersky Lab or its related entities, or using any such hardware, software, or services in the development of data or deliverables first produced in the performance of the contract. The contractor must also report any such hardware, software, or services discovered during contract performance; this requirement flows down to subcontractors. For clarity, the rule defines ''covered entity'' and ''covered article.'' A covered entity includes the entities described in section 1634. A covered article includes hardware, software, or services that the Federal Government will use on or after October 1, 2018.

As the Government considers additional actions to implement section 1634, DoD, GSA, and NASA especially welcome input on steps that the Government could take to better identify and reduce the burden on contractors related to identifying covered articles. For example:

- Is the prohibition scoped appropriately to protect the Government by including situations in which covered articles may be used in the development of data or deliverables first produced during contract performance, for example, under a systems development contract?
- Are the Government's analysis and estimates in sections VI and VII, including the estimate that 5 percent of contractors would be required to submit reports in accordance with the clause, reasonable? How could these estimates be improved?
- If the Government were to consider establishing a list to publicly share information regarding products identified as meeting the definition of a covered article (*i.e.,* excluded products), including those offered by third parties:
- What protocols should the Government apply prior to placing a product on the excluded list (*e.g.,* who should be reaching out, and to whom)?
- Should different protocols apply depending on whether the product is made by the original equipment manufacturer, sold by a reseller, or customized by a firm?
- When is it appropriate to leave a product on the excluded list indefinitely (*e.g.,* to provide notice for those who have previously acquired the product)?
- Are there steps that the Government can take to avoid inappropriately affecting the producer's interests (*e.g.,* allowing the firm to demonstrate that there is a new version

of the product that is free from concern and annotating the list accordingly)?

III. Applicability to Contracts at or Below the Simplified Acquisition Threshold and for Commercial Items, Including Commercially Available Off-the-Shelf Items

This rule adds a new contract clause at 52.204–23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities, in order to implement section 1634 of the NDAA for FY 2018. Section 1634 of this law prohibits the use of hardware, software, and services developed or provided by Kaspersky Lab and related entities by the Federal Government on or after October 1, 2018.

A. Applicability to Contracts at or Below the Simplified Acquisition Threshold

41 U.S.C. 1905 governs the applicability of laws to acquisitions at or below the simplified acquisition threshold (SAT). Section 1905 generally limits the applicability of new laws when agencies are making acquisitions at or below the SAT, but provides that such acquisitions will not be exempt from a provision of law if: (i) The law contains criminal or civil penalties; (ii) the law specifically refers to 41 U.S.C. 1905 and states that the law applies to contracts and subcontracts in amounts not greater than the SAT; or (iii) the FAR Council makes a written determination and finding that it would not be in the best interest of the Federal Government to exempt contracts and subcontracts in amounts not greater than the SAT from the provision of law.

B. Applicability to Contracts for the Acquisition of Commercial Items, Including Commercially Available Off-the-Shelf Items

41 U.S.C. 1906 governs the applicability of laws to contracts for the acquisition of commercial items, and is intended to limit the applicability of laws to contracts for the acquisition of commercial items. Section 1906 provides that if a provision of law contains criminal or civil penalties, or if the FAR Council makes a written determination that it is not in the best interest of the Federal Government to exempt commercial item contracts, the provision of law will apply to contracts for the acquisition of commercial items.

Finally, 41 U.S.C. 1907 states that acquisitions of commercially available off-the-shelf (COTS) items will be exempt from a provision of law unless the law (i) contains criminal or civil penalties; (ii) specifically refers to 41 U.S.C. 1907 and states that the law applies to acquisitions of COTS items; (iii) concerns authorities or responsibilities under the Small Business Act (15 U.S.C. 644) or bid protest procedures developed under the authority of 31 U.S.C. 3551 *et seq.,* 10 U.S.C. 2305(e) and (f), or 41 U.S.C. 3706 and 3707; or (iv) the Administrator for Federal Procurement Policy makes a written determination and finding that it would not be in the best interest of the Federal Government to exempt contracts for the procurement of COTS items from the provision of law.

C. Determinations

The FAR Council has determined that it is in the best interest of the Government to apply the rule to contracts at or below the SAT and for the acquisition of commercial items. The Administrator for Federal Procurement Policy has determined that it is in the best interest of the Government to apply this rule to contracts for the acquisition of COTS items.

While the law does not specifically address acquisitions of commercial items, including COTS items, there is an unacceptable level of risk for the Government in buying hardware, software, or services developed or provided in whole or in part by Kaspersky Lab. This level of risk is not alleviated by the fact that the item being acquired has been sold or offered for sale to the general public, either in the same form or a modified form as sold to the Government (*i.e.,* that it is a commercial item or COTS item), nor by the small size of the purchase (*i.e.,* at or below the SAT). As a result, agencies may face increased exposure for violating the law and unknowingly acquiring a covered article absent coverage of these types of acquisitions by this rule.

IV. Executive Orders 12866 and 13563

Executive Orders (E.O.s) 12866 and 13563 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). E.O. 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. This rule has been designated a ''significant regulatory action'' under Executive Order 12866. Accordingly, the Office of Management and Budget (OMB) has reviewed this rule. This rule is not a major rule under 5 U.S.C. 804.

V. Executive Order 13771

This rule is not subject to the requirements of E.O. 13771 because the rule is issued with respect to a national security function of the United States.

VI. Regulatory Flexibility Act

The change may have a significant economic impact on a substantial number of small entities within the meaning of the Regulatory Flexibility Act 5 U.S.C. 601 *et seq.* The Initial Regulatory Flexibility Analysis (IRFA) is summarized as follows:

The objective of the rule is to prescribe appropriate policies and procedures to enable agencies to determine and ensure that they are not purchasing products and services of Kaspersky Lab and its related entities for use by the Government on or after October 1, 2018. The legal basis for the rule is section 1634 of the NDAA for FY 2018, which prohibits Government use of such products on or after that date.

Data from the Federal Procurement Data System (FPDS) for FY 2017 has been used as the basis for estimating the number of contractors that may be affected by this rule. Approximately 97,632 unique entities received new awards in Fiscal Year (FY) 2017. Of these entities, 72,447 (74 percent) unique small entities received awards during 2017. It is estimated that the reports required by this rule will be submitted by 5 percent of contractors, or 3,623 small entities.

The rule requires contractors and subcontractors that are subject to the clause to report to the contracting officer, or for DoD, to the website listed in the clause, any discovery of a covered article during the course of contract performance.

The rule does not duplicate, overlap, or conflict with any other Federal rules.

Because of the nature of the prohibition enacted by section 1634, it is not possible to establish different compliance or reporting requirements or timetables that take into account the resources available to small entities or to exempt small entities from coverage of the rule, or any part thereof. DoD, GSA, and NASA were unable to identify any alternatives that would reduce the burden on small entities and still meet the objectives of section 1634.

The Regulatory Secretariat has submitted a copy of the IRFA to the Chief Counsel for Advocacy of the Small Business Administration. A copy of the IRFA may be obtained from the Regulatory Secretariat. DoD, GSA, and NASA invite comments from small business concerns and other interested parties on the expected impact of this rule on small entities.

DoD, GSA, and NASA will also consider comments from small entities concerning the existing regulations in subparts affected by this rule in accordance with 5 U.S.C. 610. Interested

parties must submit such comments separately and should cite 5 U.S.C. 610 (FAR Case 2018–010) in correspondence.

VII. Paperwork Reduction Act

The Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*) (PRA) provides that an agency generally cannot conduct or sponsor a collection of information, and no person is required to respond to nor be subject to a penalty for failure to comply with a collection of information, unless that collection has obtained Office of Management and Budget (OMB) approval and displays a currently valid OMB Control Number.

DoD, GSA, and NASA requested and OMB authorized emergency processing of an information collection involved in this rule, as OMB Control Number 9000–0197, consistent with 5 CFR 1320.13. DoD, GSA, and NASA have determined the following conditions have been met:

a. The collection of information is needed prior to the expiration of time periods normally associated with a routine submission for review under the provisions of the Paperwork Reduction Act, in view of the deadline for this provision of the NDAA which was signed into law in December 2017 and requires action before the prohibition goes into effect on October 1, 2018.

b. The collection of information is essential to the mission of the agencies to ensure the Federal Government does not purchase prohibited articles, and can respond appropriately if any such articles are not identified until after delivery or use.

c. The use of normal clearance procedures would prevent the collection of information from contractors, for national security purposes, as discussed in section VIII of this preamble.

Passage of the omnibus appropriations bill and the availability of additional funding for FY 18 has increased agency purchasing activity, and the information to be collected is necessary to ensure that this purchasing is done responsibly and consistent with national security.

Moreover, DoD, GSA, and NASA cannot comply with the normal clearance procedures because public harm is reasonably likely to result if current clearance procedures are followed. Not only would agencies be more likely to purchase and install prohibited items, but even if such items were identified prior to the October 1 date, agencies would incur substantial additional costs replacing such items, as well as additional administrative costs for reprocurement.

DoD, GSA, and NASA intend to provide separate 60-day notice in the **Federal Register** requesting public comment on the information collection contained within this rule.

Agency: DoD, GSA, and NASA.

Type of Information Collection: New Collection.

Title of Collection: Use of Products and Services of Kaspersky Lab.

Affected Public: Private Sector—Business.

Total Estimated Number of Respondents: 4,882.

Average Responses per Respondents: 5.

Total Estimated Number of Responses: 24,410.

Average Time per Response: 1.5 hour.

Total Annual Time Burden: 36,615.

OMB Control Number: 9000–0197.

The public reporting burden for this collection of information consists of reports of identified covered articles during contract performance as required by 52.204–23. Reports are estimated to average 1.5 hour per response, including the time for reviewing definitions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the report.

The subsequent 60-day notice published by DoD, GSA, and NASA will invite public comments.

VIII. Determination To Issue an Interim Rule

A determination has been made under the authority of the Secretary of Defense (DoD), Administrator of General Services (GSA), and the Administrator of the National Aeronautics and Space Administration (NASA) that urgent and compelling reasons exist to promulgate this interim rule without prior opportunity for public comment. It is critical that the FAR is immediately revised to include the requirements of the law, which prohibits the Federal Government from using hardware, software, or services of Kaspersky Lab and its related entities on or after October 1, 2018.

Although this prohibition does not apply until October 1, 2018, agencies and contractors must begin to take steps immediately to meet this deadline. In this regard, covered articles include hardware, software, and services acquired before October 1, 2018, that the Federal Government will use on or after October 1, 2018. Because so many IT products and services are used for more than a few months, it is critical that contractors be placed on notice as soon as possible of this prohibition so that agencies can ensure that they comply with the law and avoid acquisitions of covered articles that the Government will continue to use on or after October 1, 2018. Pursuant to 41 U.S.C. 1707 and FAR 1.501–3(b), DoD, GSA, and NASA will consider public comments received in response to this interim rule in the formation of the final rule.

List of Subject in 48 CFR Parts 1, 4, 13, 39, and 52

Government procurement.

Dated: June 7, 2018.

William F. Clark,

Director, Office of Governmentwide Acquisition Policy, Office of Acquisition Policy, Office of Governmentwide Policy.

Therefore, DoD, GSA, and NASA amend 48 CFR parts 1, 4, 13, 39, and 52 as set forth below:

■ 1. The authority citation for 48 CFR parts 1, 4, 13, 39, and 52 continues to read as follows:

Authority: 40 U.S.C. 121(c); 10 U.S.C. chapter 137; and 51 U.S.C. 20113.

PART 1—FEDERAL ACQUISITION REGULATIONS SYSTEM

1.106 [Amended]

■ 2. Amend section 1.106 by adding to the table, in numerical sequence, FAR segment ''52.204–23'' and its corresponding OMB control number ''9000–0197''.

PART 4—ADMINISTRATIVE MATTERS

■ 3. Add subpart 4.20 to read as follows:

SUBPART 4.20—PROHIBITION ON CONTRACTING FOR HARDWARE, SOFTWARE, AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB

Sec.

SUBPART 4.20—PROHIBITION ON CONTRACTING FOR HARDWARE, SOFTWARE, AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB

4.2001 Definitions

As used in this subpart—

Covered article means any hardware, software, or service that—

(1) Is developed or provided by a covered entity;

(2) Includes any hardware, software, or service developed or provided in whole or in part by a covered entity; or

(3) Contains components using any hardware or software developed in whole or in part by a covered entity.

Covered entity means—

(1) Kaspersky Lab;
(2) Any successor entity to Kaspersky Lab;
(3) Any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or
(4) Any entity of which Kaspersky Lab has a majority ownership.

4.2002 Prohibition.

Section 1634 of Division A of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115–91) prohibits Government use on or after October 1, 2018, of any hardware, software, or services developed or provided, in whole or in part, by a covered entity. Contractors are prohibited from—
(a) Providing any covered article that the Government will use on or after October 1, 2018; and
(b) Using any covered article on or after October 1, 2018, in the development of data or deliverables first produced in the performance of the contract.

4.2003 Notification.

When a contractor provides notification pursuant to 52.204–23, follow agency procedures.

4.2004 Contract clause.

The contracting officer shall insert the clause at 52.204–23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities, in all solicitations and contracts.

PART 13—SIMPLIFIED ACQUISITION PROCEDURES

■ 4. Amend section 13.201 by adding paragraph (i) to read as follows:

13.201 General.

* * * * *

(i) Do not purchase any hardware, software, or services developed or provided by Kaspersky Lab that the Government will use on or after October 1, 2018. (See 4.2002.)

PART 39—ACQUISITION OF INFORMATION TECHNOLOGY

■ 5. Amend section 39.101 by adding paragraph (e) to read as follows:

39.101 Policy.

* * * * *

(e) Contracting officers shall not purchase any hardware, software, or services developed or provided by Kaspersky Lab that the Government will use on or after October 1, 2018. (See 4.2002.)

PART 52—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

■ 6. Add section 52.204–23 to read as follows:

52.204–23 Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities.

As prescribed in 4.2004, insert the following clause:

Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018)

(a) *Definitions.* As used in this clause—
Covered article means any hardware, software, or service that—
(1) Is developed or provided by a covered entity;
(2) Includes any hardware, software, or service developed or provided in whole or in part by a covered entity; or
(3) Contains components using any hardware or software developed in whole or in part by a covered entity.
Covered entity means—
(1) Kaspersky Lab;
(2) Any successor entity to Kaspersky Lab;
(3) Any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or
(4) Any entity of which Kaspersky Lab has a majority ownership.
(b) *Prohibition.* Section 1634 of Division A of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115–91) prohibits Government use of any covered article. The Contractor is prohibited from—
(1) Providing any covered article that the Government will use on or after October 1, 2018; and
(2) Using any covered article on or after October 1, 2018, in the development of data or deliverables first produced in the performance of the contract.
(c) *Reporting requirement.* (1) In the event the Contractor identifies a covered article provided to the Government during contract performance, or the Contractor is notified of such by a subcontractor at any tier or any other source, the Contractor shall report, in writing, to the Contracting Officer or, in the case of the Department of Defense, to the website at *https://dibnet.dod.mil.* For indefinite delivery contracts, the Contractor shall report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at *https://dibnet.dod.mil.*
(2) The Contractor shall report the following information pursuant to paragraph (c)(1) of this clause:
(i) Within 1 business day from the date of such identification or notification: The contract number; the order number(s), if applicable; supplier name; brand; model number (Original Equipment Manufacturer (OEM) number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.
(ii) Within 10 business days of submitting the report pursuant to paragraph (c)(1) of this clause: Any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of a covered article, any reasons that led to the use or submission of the covered article, and any additional efforts that will be incorporated to prevent future use or submission of covered articles.
(d) *Subcontracts.* The Contractor shall insert the substance of this clause, including this paragraph (d), in all subcontracts, including subcontracts for the acquisition of commercial items.

(End of clause)

■ 7. Amend section 52.212–5 by—
■ a. Revising the date of the clause;
■ b. Redesignating paragraphs (a)(2) through (4) as paragraphs (a)(3) through (5), respectively, and adding a new paragraph (a)(2);
■ c. Redesignating paragraphs (e)(1)(iii) through (xxi) as paragraphs (e)(1)(iv) through (xxii), respectively, and adding a new paragraph (e)(1)(iii); and
■ d. In Alternate II:
■ i. Revising the date of the alternate; and
■ ii. Redesignating paragraphs (e)(1)(ii)(C) through (S) as paragraphs (e)(1)(ii)(D) through (T), respectively, and adding a new paragraph (e)(1)(ii)(C).

The revisions and additions read as follows:

52.212–5 Contract Terms and Conditions Required To Implement Statutes or Executive Orders—Commercial Items.

* * * * *

Contract Terms and Conditions Required To Implement Statutes or Executive Orders—Commercial Items (Jul 2018)

* * * * *

(a) * * *

____ (2) 52.204–23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018) (Section 1634 of Pub. L. 115–91).

* * * * *

(e)(1) * * *

(iii) 52.204–23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018) (Section 1634 of Pub. L. 115–91).

* * * * *

Alternate II (Jul 2018). * * *

* * * * *

(e)(1) * * *

(ii) * * *

(C) 52.204–23, Prohibition on Contracting for Hardware, Software, and Services

Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018) (Section 1634 of Pub. L. 115–91).

* * * * *

■ 8. Amend section 52.213–4 by—

■ a. Revising the date of the clause; and

■ b. Redesignating paragraphs (a)(1)(ii) through (vii) as paragraphs (a)(1)(iii) through (viii), respectively, and adding a new paragraph (a)(1)(ii).

The revision and addition read as follows:

52.213–4 Terms and Conditions—Simplified Acquisitions (Other Than Commercial Items).

* * * * *

Terms and Conditions—Simplified Acquisitions (Other than Commercial Items) (Jul 2018)

(a) * * *

(1) * * *

(ii) 52.204–23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018) (Section 1634 of Pub. L. 115–91).

* * * * *

■ 9. Amend section 52.244–6 by—

■ a. Revising the date of the clause;

■ b. Redesignating paragraphs (c)(1)(iv) through (xviii) as paragraphs (c)(1)(v) through (xix), respectively, and adding a new paragraph (c)(1)(iv).

The revision and addition read as follows:

52.244–6 Subcontracts for Commercial Items.

* * * * *

Subcontracts for Commercial Items (Jul 2018)

* * * * *

(c)(1) * * *

(iv) 52.204–23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018) (Section 1634 of Pub. L. 115–91).

* * * * *

[FR Doc. 2018–12847 Filed 6–14–18; 8:45 am]

BILLING CODE 6820–EP–P

DEPARTMENT OF DEFENSE

GENERAL SERVICES ADMINISTRATION

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

48 CFR Parts 1, 9, 12, 13, and 52

[FAC 2005–99; FAR Case 2017–018; Item II; Docket No. 2017–0018, Sequence No. 1]

RIN 9000–AN57

Federal Acquisition Regulation: Violations of Arms Control Treaties or Agreements With the United States

AGENCY: Department of Defense (DoD), General Services Administration (GSA), and National Aeronautics and Space Administration (NASA).

ACTION: Interim rule.

SUMMARY: DoD, GSA, and NASA are issuing an interim rule amending the Federal Acquisition Regulation (FAR) to implement a section of the National Defense Authorization Act for Fiscal Year 2017 that addresses measures against persons involved in activities that violate arms control treaties or agreements with the United States.

DATES:

Effective: June 15, 2018.

Comment Date: Interested parties should submit written comments to the Regulatory Secretariat Division at one of the addresses shown below on or before August 14, 2018 to be considered in the formation of the final rule.

ADDRESSES: Submit comments in response to FAC 2005–99, FAR Case 2017–018, by any of the following methods:

- *Regulations.gov: http://www.regulations.gov.* Submit comments via the Federal eRulemaking portal by searching for ''FAR Case 2017–018.'' Select the link ''Comment Now'' that corresponds with ''FAR Case 2017–018.'' Follow the instructions provided on the screen. Please include your name, company name (if any), and ''FAR Case 2017–018'' on your attached document.
- *Mail:* General Services Administration, Regulatory Secretariat Division (MVCB), ATTN: Ms. Lois Mandell, 1800 F Street NW, 2nd Floor, Washington, DC 20405.

Instructions: Please submit comments only and cite FAC 2005–99, FAR Case 2017–018, in all correspondence related to this case. All comments received will be posted without change to *http://www.regulations.gov,* including any personal and/or business confidential information provided. To confirm receipt of your comment(s), please check *www.regulations.gov,* approximately two to three days after submission to verify posting (except allow 30 days for posting of comments submitted by mail).

FOR FURTHER INFORMATION CONTACT: Ms. Cecelia L. Davis, Procurement Analyst, at 202–219–0202 for clarification of content. For information pertaining to status or publication schedules, contact the Regulatory Secretariat Division at 202–501–4755. Please cite FAC 2005–99, FAR Case 2017–018.

SUPPLEMENTARY INFORMATION:

I. Background

This interim rule amends the FAR to implement a section of the National Defense Authorization Act (NDAA) for Fiscal Year 2017 that addresses measures against persons involved in activities that violate arms control treaties or agreements with the United States. This rule amends FAR part 9, Contractor Qualifications, and adds a provision at FAR 52.209–13 to implement section 1290 of the National Defense Authorization Act for Fiscal Year 2017 (Pub. L. 114–328), codified at 22 U.S.C. 2593e.

The President submits annually to Congress a report prepared by the Secretary of State with the concurrence of the Director of Central Intelligence and in consultation with the Secretary of Defense, the Secretary of Energy, and the Chairman of the Joint Chiefs of Staff, on the status of United States policy and actions with respect to arms control, nonproliferation, and disarmament, pursuant to section 403 of the Arms Control and Disarmament Act (22 U.S.C. 2593a). In this report, the Secretary of State assesses adherence to and compliance with arms control, nonproliferation, and disarmament agreements and commitments by the United States and other countries. This report is submitted in unclassified form, with classified annexes, as appropriate. The Department of State's most recent unclassified report submitted in April 2018 to Congress is available at *https://www.state.gov/t/avc/rls/rpt/.*

The Secretary of the Treasury is required to submit to the appropriate Congressional committees a report, consistent with the protection of intelligence sources and methods, identifying every person with respect to whom there is credible information indicating that the person is—

- An individual who is a citizen, national, or permanent resident of, or an entity organized under the laws of, a noncompliant country; and