UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

KASPERSKY LAB, INC. and KASPERSKY LABS LIMITED, 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, Appellees.	Case Nos. 18-5176 & 18-5177

APPELLANTS' EMERGENCY MOTION TO STAY

Pursuant to 28 U.S.C. § 1657, and D.C. Circuit Rules 8 and 27, Appellants Kaspersky Lab, Inc. and Kaspersky Labs Limited (collectively, "Kaspersky Lab") respectfully move for an emergency stay of Sections 1634(a) and (b) of the National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91 (the "NDAA"), the interim rule that accelerates implementation of Section 1634(a), and any other federal regulation to implement Section 1634(a). Section 1634(a) of the NDAA prohibits the federal government from using "any hardware, software, or services developed or provided, in whole or in part" by Kaspersky Lab. Under Section 1634(b), that prohibition takes effect on October 1, 2018.

The federal government is now accelerating the effective date of Section 1634(a) to July 16, 2018. 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 directing implementation of Section 1634(a) of the NDAA, effective July 16, 2018, without prior opportunity for public comment.

Kaspersky Lab respectfully requests that the Court stay implementation of Sections 1634(a) and (b) of the NDAA, the interim rule, and any implementing regulations before July 16, 2018, and until this Court resolves on the merits Kaspersky Lab's lawsuit asserting that Section 1634(a) is an unconstitutional bill of attainder. Kaspersky Lab has notified the Clerk of the Court and opposing counsel of this motion by telephone. Kaspersky Lab also requests disposition of this emergency motion before July 16, 2018. In the event the Court declines to grant emergency relief before July 16, 2018, Kaspersky Lab requests that this Court consider this motion for a stay at oral argument on September 14, 2018.

BACKGROUND

Kaspersky Lab is a multinational cybersecurity company exclusively focused on protecting against cyberthreats, no matter their origin. J.A. 142 ¶ 18. It is one of the world's largest privately owned cybersecurity companies. *Id.*

The BOD

On September 13, 2017, without prior opportunity for public comment, the Department of Homeland Security issued Binding Operational Directive 17-01 (the "BOD"), 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 BOD also states that "[t]his 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." *Id.* The Department of Homeland Security finalized the BOD on December 6, 2017. *See* J.A. 126–29.

The NDAA

On July 27, 2017, Senator Jeanne Shaheen proposed an amendment to the NDAA that prohibited the U.S. 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," J.A. 158, and "a wider threat" than

Russia's interference in a presidential election, *see id.* She 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," *id.* at 156. She 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 singled out Kaspersky Lab in the NDAA and prohibited the federal government from using its software, hardware, and services. Section 1634 of the NDAA states, 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.

Section 1634(a) is a more sweeping prohibition than the BOD, because it prohibits the federal government and federal contractors from using "any . . . software, or services developed or provided, in whole or in part, by . . . Kaspersky Lab" and its affiliates, including embedded code, threat intelligence, and security training services that were excepted from the BOD. Kaspersky Lab argues that this provision of the NDAA constitutes an unconstitutional bill of attainder.

Procedural History

Kaspersky Lab filed two lawsuits in the District Court: the first, against the Department of Homeland Security and its Secretary (case no. 1:17-cv-02697 (CKK)) (the "APA Case"), challenged the BOD, which the Department finalized on December 6, 2017, and which required all federal departments and agencies to identify and begin removing all "Kaspersky-branded products" within 90 days. *See* J.A. 1. The second, against the federal government, sought invalidation of Sections 1634(a) and (b) of the NDAA (case no. 1:18-cv-00325 (CKK)) (the "Bill of Attainder Case"), which include a broader ban on all Kaspersky Lab goods and services. *See id.* at 138.

On May 30, 2018, the District Court issued a consolidated memorandum opinion in the two cases. *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); J.A. 169–223 (memorandum opinion). The District Court dismissed the

Bill of Attainder Case for failure to state a claim on which relief could be granted and dismissed the APA Case for lack of standing. J.A. 223.

Kaspersky Lab's notice of appeal was docketed in this Court on June 8, 2018. Later that day, Kaspersky Lab filed an unopposed emergency motion for expedited consideration and an expedited briefing schedule. By seeking expedited consideration, Kaspersky Lab sought an opportunity for this Court to rule on the merits of the appeal before Section 1634(a) becomes effective on October 1. On June 12, this Court granted that motion, setting the following deadlines:

Appellants' Brief	June 27, 2018
Appendix	June 27, 2018
Appellees' Brief	July 30, 2018
Appellants' Reply Brief	August 13, 2018

On June 15, the Clerk of the Court scheduled oral argument for September 14.

The Interim Rule

Also on June 15, 2018, three days after this Court granted the motion to expedite the appeal, the Department of Defense, the General Services Administration, and the National Aeronautics and Space Administration published an interim rule: Federal Acquisition Regulation; Use of Products and Services of Kaspersky Lab, 83 Fed. Reg. 28,141 (June 15, 2018) (the "interim rule"). The interim rule states that it is intended "to implement section 1634 of the NDAA," *id.*

at 28,142, and that "urgent and compelling reasons exist to promulgate this interim rule without prior opportunity for public comment," *id.* at 28,143. The interim rule observes: "Although [the] prohibition [in Section 1634(a) of the NDAA] does not apply until October 1, 2018, agencies and contractors must begin to take steps immediately to meet this deadline." *Id.* On or after July 16, 2018, "[federal] [c]ontracting officers" must include in solicitations and must modify existing contracts to include the prohibition from Section 1634(a) on using hardware, software, or services from Kaspersky Lab and its affiliates. *See id.* at 28,141.[1]

For all practical purposes, the interim rule accelerates Section 1634(a)'s effective date from October 1 to July 16. Kaspersky Lab therefore respectfully requests that this Court enjoin Sections 1634(a) and (b) of the NDAA, the interim rule, and any other federal regulations that seek to implement Section 1634(a). Kaspersky Lab requests that such an injunction issue by July 16 and remain in place until this Court resolves the merits of the Bill of Attainder Case.

ARGUMENT

Sections 1634(a) and (b) of the NDAA and any federal regulations implementing those provisions should be stayed, because (1) Kaspersky Lab is

---

1. On June 22, 2018, the same agencies solicited comments regarding the collection of information associated with the interim rule. *See* Information Collection; Use of Products and Services of Kaspersky Lab, 83 Fed. Reg. 29,116 (June 22, 2018).

likely to prevail on the merits of its Bill of Attainder Case; (2) Kaspersky Lab will face irreparable harm if relief is withheld; (3) there will not be substantial harm to other parties if relief is granted; and (4) the public interest favors such relief. *See* D.C. Cir. R. 8(a)(1). Because doing so would be impracticable, Kaspersky Lab has not moved for a stay in the District Court. *See* Fed. R. App. P. 8(a)(2)(A)(i).

I. Kaspersky Lab has met the standard for emergency relief.

This Court considers four factors when deciding whether emergency relief is warranted: "(i) the likelihood that the moving party will prevail on the merits; (ii) the prospect of irreparable injury to the moving party if relief is withheld; (iii) the possibility of harm to other parties if relief is granted; and (iv) the public interest." D.C. Cir. R. 8(a)(1). The four factors need not be equally strong: "If the arguments for one factor are particularly strong, an injunction may issue even if the arguments in other areas are rather weak." *Mills v. District of Columbia*, 571 F.3d 1304, 1308 (D.C. Cir. 2009) (quoting *CityFed Fin. Corp. v. Office of Thrift Supervision*, 58 F.3d 738, 747 (D.C. Cir. 1995)). For example, in *Mills*, this Court held that appellants had "established the requisites for the granting of a preliminary injunction" by showing only the first two factors. *Id.* at 1312. Some showing of the second factor is crucial, because "the basis of injunctive relief in the federal courts has always been irreparable harm." *CityFed Fin. Corp.*, 58 F.3d at 747 (citation omitted).

A. Kaspersky Lab will likely prevail on the merits of its Bill of Attainder Case.

Kaspersky Lab will likely prevail on its claim that Section 1634(a) of the NDAA is an unconstitutional bill of attainder. Article I, Section 9 of the U.S. Constitution prohibits Congress from passing bills of attainder. "[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)). There is no dispute that Section 1634(a) applies with specificity to Kaspersky Lab: Section 1634(a) is titled "PROHIBITION ON USE OF PRODUCTS AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB."

Courts reviewing whether a legislative act imposes punishment 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 v. Adm'r of Gen. Servs.*, 433 U.S. 425, 473, 475–76 (1977)).

Kaspersky Lab is likely to succeed because all three tests point to a finding that Section 1634(a) punishes the company.

1. Section 1634(a) imposes punishment under the historical test.

First, Section 1634(a) is legislative punishment under the historical test because it singles out Kaspersky Lab and uniquely brands it with infamy and disloyalty. "[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). When Congress "designates in no uncertain terms the persons who possess [] feared characteristics," rather than "set[ting] forth a generally applicable rule" applying to any persons who possess those characteristics, it "exceed[s] its authority." *United States v. Brown*, 381 U.S. 437, 450 (1965). Section 1634(a) applies with specificity to Kaspersky Lab, marking Kaspersky Lab as disloyal and lending, as the District Court admitted, "the imprimatur of government authority" to the assertion that Kaspersky Lab is not to be trusted. *See Kaspersky Lab, Inc.*, 2018 WL 2433583, at *25 (internal quotation marks omitted).

Moreover, Section 1634(a) is consistent with historical forms of legislative punishment. In *Ex parte Garland*, 71 U.S. (4 Wall.) 333, 377 (1867), *United States v. Lovett*, 328 U.S. 303, 315–16 (1946), and *United States v. Brown*, 381 U.S. 437, 449–50 (1965), the Supreme Court rejected as bills of attainder statutes

that, respectively: prohibited Confederates from being admitted to the bar and serving as attorneys; prohibited the federal government from paying certain employees believed to be "subversives" who had been working for the government for years; and 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 "[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 v. Missouri*, 71 U.S. (4 Wall.) 277, 320 (1867)). As the *Lovett* Court observed, "permanent proscription from any opportunity to serve the Government is punishment, and of a most severe type." 328 U.S. at 316 (citations omitted).

Conversely, in the cases in which this Court has declined to declare a legislative enactment punitive, the enactment has been temporary or escapable. *See BellSouth v. FCC*, 144 F.3d 58, 65 (D.C. Cir. 1998) ("*Bell South I*"); *BellSouth Corp. v. FCC*, 162 F.3d 678, 685 (D.C. Cir. 1998) ("*Bell South II*"); *Siegel v. Lyng*, 851 F.2d 412, 416–18 (D.C. Cir. 1988). Section 1634(a) permanently disqualifies a single entity from any commerce with the U.S. Government, and because Section 1634(a) deems Kaspersky Lab a cyberthreat, it has the practical result of barring Kaspersky Lab from doing business as a cybersecurity company. Section 1634(a) contains no limiting provisions, in time or scope, and no appeal mechanism or

other ways it can be overcome. It is a "permanent proscription" that is thus punitive.

2. Section 1634(a) imposes punishment under the functional test.

Second, the type and severity of the burdens that Section 1634(a) imposes do not further nonpunitive legislative purposes. 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. "Punitive purposes, however rational, don't count." *Id.* To be nonpunitive, there should be some parity between the burden and the asserted nonpunitive purpose. "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." *Foretich*, 351 F.3d at 1222. As a consequence, "the availability of less burdensome alternatives" to achieve the purported nonpunitive purposes "can . . . cast doubt on purported nonpunitive purposes." *Id*. (internal quotation marks omitted) (citing *Nixon*, 433 U.S. at 482). Cases such as this require extra vigilance, because "[t]he 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) (citation omitted).

As the Supreme Court noted in *Lovett*, permanently barring a person or entity from a specific vocation or from government service is punishment "of a

most severe type." 328 U.S. at 316. Therefore, the permanent, inescapable embargo on Kaspersky Lab from providing any product or service to the U.S. Government is a very grave burden. That burden is disproportionate to the professed nonpunitive "national security" justification because there are less burdensome alternatives to total and permanent legislative debarment. That Congress chose not to pursue less-burdensome paths indicates that the purpose of Section 1634(a) was to punish Kaspersky Lab.

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. *See BellSouth II*, 162 F.3d at 691. In *BellSouth II*, this Court ruled that a law was not punitive because the apparent targets were "no worse off" than they had been under a prior settlement, "and there are many who think their position has vastly improved." *Id.* Kaspersky Lab is challenging both Section 1634(a) and the BOD, and so the relevant comparison is between Kaspersky Lab's status today and its status before the BOD. Even if the relevant comparison were to Kaspersky Lab's status after the BOD, the change would be significant and negative. Section 1634(a) imposed harsh additional burdens on Kaspersky Lab, including reputational harm from the all-encompassing ban on Kaspersky Lab products and services; fiscal harm, in the further loss of customers; and constitutional harm, as the target of a bill of attainder.

3. Section 1634(a) imposes punishment under the motivational test.

Third, legislative history evinces a congressional intent to adjudge and punish Kaspersky Lab through the enactment of Section 1634(a). "[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." *Foretich*, 351 F.3d 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 *Brown*, 381 U.S. at 453–54). The statements of a bill's sponsor can "provide evidence of Congress' intent" when they "are consistent with the statutory language and other legislative history." *See Brock v. Pierce County*, 476 U.S. 253, 263 (1986) (citing *Grove City Coll. v. Bell*, 465 U.S. 555, 567 (1984)).[2]

The sponsor of Section 1634(a), Senator Jeanne Shaheen, has made public statements demonstrating a congressional intent to punish Kaspersky Lab. Senator Shaheen penned a September 4, 2017 *New York Times* editorial about Kaspersky Lab titled: "The Russian Company That Is a Danger to Our Security." J.A. 156. Senator Shaheen publicized that Kaspersky Lab is "a threat to our national

---

2. *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.").

security," *id.* at 158, and "a wider threat" than Russia's interference in a presidential election, *see id.* She claimed that the federal government's use of Kaspersky Lab software was "already a huge breach of national security data," and "Congress has serious doubts about the company." *See id.* 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." *Id.*

Nothing in the legislative history contradicts the public statements on Section 1634(a) made by the legislative sponsor. *See Brock*, 476 U.S. at 263. Those statements are also consistent with the plain text of the statute, which singles out Kaspersky Lab and no other specific entities, and they evince "a congressional purpose to behave like a court" and to find guilt.

B. Implementing Section 1634(a) before the merits of the Bill of Attainder Case have been resolved will cause Kaspersky Lab irreparable harm.

Premature implementation of Section 1634(a) will cause irreparable harm to Kaspersky Lab in two ways: First, the implementation of a bill of attainder is a continued violation of Kaspersky Lab's constitutional rights, and second, implementation of Section 1634(a) will cause irreparable financial and reputational harm to Kaspersky Lab.

1. Allowing a bill of attainder to become effective is an irreparable violation of Kaspersky Lab's constitutional rights.

Targeting Kaspersky Lab via an unconstitutional legislative punishment is in itself an irreparable harm. "'[S]uits for declaratory and injunctive relief against the threatened invasion of a constitutional right do not ordinarily require proof of any injury other than the threatened constitutional deprivation itself.' Thus . . . 'a prospective violation of a constitutional right constitutes irreparable injury for these purposes.'" *Gordon v. Holder*, 721 F.3d 638, 653 (D.C. Cir. 2013) (internal citation omitted); *see also Mills*, 571 F.3d at 1312 ("It has long been established that the loss of constitutional freedoms, 'for even minimal periods of time, unquestionably constitutes irreparable injury.'" (citation omitted)). The prospect that Kaspersky Lab might continue to be subject to legislative punishment is a constitutional harm that suffices to show irreparable injury.

2. The prospect of implementing Section 1634(a) has caused and will continue to cause Kaspersky Lab irreparable financial and reputational harm.

Section 1634(a) has caused and will continue to cause irreparable economic harm, through both loss of customers and reputational injury. Kaspersky Lab is likely unable to recover monetary damages from the federal government in the Bill of Attainder or APA Cases. *See Lane v. Pena*, 518 U.S. 187, 192–93 (1996) (plaintiff could not pursue claims for money damages against the government

because statute did not expressly waive federal government's sovereign immunity with respect to such claims); *Cohen v. United States*, 650 F.3d 717, 723 (D.C. Cir. 2011) (en banc) (APA authorizes suits against the government "in actions not seeking money damages"). "In the context of preliminary injunctions, numerous courts have held that the inability to recover monetary damages because of sovereign immunity renders the harm suffered irreparable." *Odebrecht Constr. v. Sec'y, Fla. DOT*, 715 F.3d 1268, 1289 (11th Cir. 2013); *see Chamber of Commerce v. Edmondson*, 594 F.3d 742, 770–71 (10th Cir. 2010); *Iowa Utils. Bd. v. FCC*, 109 F.3d 418, 426 (8th Cir. 1996).

Kaspersky Lab's losses from Section 1634(a) are significant. Although Kaspersky Lab's contracts with the U.S. Government do not account for a large portion of its annual revenue, "[t]he U.S. has been, and remains, one of the most significant geographic markets in Kaspersky Lab's global business." J.A. 143 ¶ 22. "Sales to customers in the United States represent approximately one quarter of total global bookings in 2016," *id.* at 7–8 ¶ 32, and Kaspersky Lab "has invested over a half a billion dollars in its operations over the last twelve years," including "over $65 million in 2016 alone," *id.* Given its presence in the U.S. market, Kaspersky Lab "has a substantial interest in its status as a vendor to the U.S. Government." *Id.* at 8 ¶ 34.

Kaspersky Lab executive Angelo Gentile explained that the company has "been receiving and processing an unprecedented volume of product return and early termination requests since the issuance of the [narrower ban in the] BOD." *See* Angelo Gentile's Decl. in Supp. of Pls.' Mot. for Summ. J. (Docket Entry 19-3) ("Gentile Decl.") 5 ¶ 20, *Kaspersky Lab, Inc. v. Dep't of Homeland Sec.*, 1:17-cv-02697 (CKK). Kaspersky Lab's business-to-business sales have also experienced "significant decline . . . resulting from both the decline in corporate customer retention and the decline in new corporate customer acquisition." *Id*. at 9 ¶ 32. Business-to-business customers who were federal contractors did not wait until final implementation of the BOD before informing Kaspersky Lab's "reseller partners of their intention to terminate their Kaspersky Lab subscriptions and demanding refunds for their terminated subscriptions." *Id*.

The loss of business and reputation caused by Section 1634(a) is even greater than that suffered under the BOD. The BOD states that "[t]his 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." 82 Fed. Reg. at 43,783. Section 1634(a), however, prohibits the federal government and federal contractors from using "any . . . software, or services developed or provided, in whole or in part, by

. . . Kaspersky Lab" and its affiliates, including embedded code, threat intelligence, and security training services. As the District Court observed:

> [Section 1634(a)] is broader in scope than BOD 17-01 in two ways. First, it applies to all Kaspersky Lab products (hardware, software, and services), whereas the BOD only applied to a smaller subset of "Kaspersky-branded products." Second, unlike BOD 17-01, the NDAA does not have any carve outs or exceptions for national security systems or other systems used by the Department of Defense or the intelligence community.

J.A. 187. Section 1634(a) and the interim rule that accelerates its effective date cause harm separate from and in addition to that caused by the BOD. *See* Gentile Suppl. Decl. 2–4 ¶¶ 2–5; Matesen Decl. 2–4 ¶¶ 3–8. The reputational and financial harm imposed by Section 1634(a) is significant and unrecoverable, and thus irreparable.

Several federal courts of appeals have recognized that a company's "loss of goodwill and reputation" can constitute irreparable harm that warrants injunctive relief. *See, e.g.*, *Stuller, Inc. v. Steak N Shake Enters., Inc.*, 695 F.3d 676, 680 (7th Cir. 2012); *Rogers Grp., Inc. v. City of Fayetteville, Arkansas*, 629 F.3d 784, 789–90 (8th Cir. 2010); *Am. Trucking Ass'ns, Inc. v. City of Los Angeles*, 559 F.3d 1046, 1058–59 (9th Cir. 2009). The reputational injury resulting from the legislature casting aspersions on a group is prohibited by the Constitution. Anthony Dick, Note, *The Substance of Punishment Under the Bill of Attainder Clause*, 63 Stan. L. Rev. 1177, 1210 (2011) ("[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.'" (quoting *Joint Anti-Fascist Refugee Comm. v. McGrath*, 341 U.S. 123, 139 (1951) (Burton, J., joined by Douglas, J.))).[3] In *Lovett*, the offending legislation "stigmatized [respondents'] reputation and seriously impaired their chance to earn a living." 328 U.S. at 314. Similarly, in *Foretich*, this Court recognized as a bill of attainder a legislative determination of criminal sexual abuse that destroyed a physician's reputation. 351 F.3d at 1220. Staying implementation of Sections 1634(a) and (b) would not remedy all harm to Kaspersky Lab's reputation, but it would prevent further harm. *See, e.g.*, *KindHearts for Charitable Humanitarian Dev., Inc. v. Geithner*, 676 F. Supp. 2d 649, 654 (N.D. Ohio 2009).

Kaspersky Lab faces the prospect that the U.S. Government's unfounded mistrust of the company will remain enshrined in U.S. law. Kaspersky Lab's position as a trusted software vendor has been compromised. It is difficult to envision a more severe injury to a company's reputation—particularly a security

3. *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).

company—than the United States government declaring the company a threat to national security and refusing to do business with it. *See* Gentile Decl. 5 ¶ 18 (The narrower ban in the BOD "has had, and continues to have, a profound impact on the Company's brand, reputation, and prospects everywhere that it does business.").

C. No third parties will suffer harm from staying the implementation of Section 1634(a).

The only third party potentially implicated by staying the effective date of Section 1634(a) is the U.S. Government, but the government "cannot suffer harm from an injunction that merely ends an unlawful practice." *Rodriguez v. Robbins*, 715 F.3d 1127, 1145 (9th Cir. 2013); *see also Open Cmtys. All. v. Carson*, 286 F. Supp. 3d 148, 179 (D.D.C. 2017). In *Open Communities Alliance*, the district court enjoined an administrative rule when the only harm to the government was speculative. 286 F. Supp. 3d at 179. The government's assertion in this case that Section 1634(a) is necessary to protect national security is similarly speculative. In November 2017, the Department of Homeland Security acknowledged publicly that it does not have conclusive evidence that Kaspersky Lab has ever facilitated the breach of any U.S. Government information system. *See* J.A. 147 ¶ 38. The lack of concrete harm to third parties contrasts with the significant harm visited on Kaspersky Lab.

D. Staying the implementation of Section 1634(a) furthers the public interest.

Staying the effective date of Section 1634(a) promotes the public interest because it prevents the United States from violating Kaspersky Lab's constitutional rights. "[E]nforcement of an unconstitutional law is always contrary to the public interest." *Gordon v. Holder*, 721 F.3d 638, 653 (D.C. Cir. 2013); *see also Lamprecht v. FCC*, 958 F.2d 382, 390 (D.C. Cir. 1992); *Preminger v. Principi*, 422 F.3d 815, 826 (9th Cir. 2005) ("Generally, public interest concerns are implicated when a constitutional right has been violated, because all citizens have a stake in upholding the Constitution.").

Thus, for example, in *Gordon*, this Court concluded that the district court did not abuse its discretion when it determined that the public's interest in protecting the Constitution outweighed its interest in enforcing the laws entered by Congress. 721 F.3d at 652–53. Similarly, in *KindHearts*, 676 F. Supp. 2d at 655, the district court entered a preliminary injunction against the designation of the plaintiff as a terrorist organization, finding that the public's interest in upholding the Constitution outweighed any public stake in the government doing its job unimpeded: "The public . . . has a fundamental and great interest in seeing the Constitution upheld and ensuring that remedies be provided when the government has acted in derogation of constitutional rights."

II. Moving first in the District Court for a stay would be impracticable.

As a general matter, "[t]he filing of a notice of appeal is an event of jurisdictional significance—it confers jurisdiction on the court of appeals and divests the district court of its control over those aspects of the case involved in the appeal." *Griggs v. Provident Consumer Disc. Co.*, 459 U.S. 56, 58 (1982) (per curiam) (citations omitted).

After Kaspersky Lab noted its appeal and this Court decided to expedite consideration of the case, the federal government published an interim rule accelerating the effective date of Section 1634(a) of the NDAA. It is doubtful, in the current posture, that the District Court would have jurisdiction to enjoin Section 1634(a) or the interim rule. Even if the District Court possessed jurisdiction to grant the relief this motion seeks, the result would be foreordained. That court already ruled, erroneously, that Kaspersky Lab has not stated a plausible claim in the Bill of Attainder Case, dubbing the company's alleged injury "exaggerated." *See* J.A. 204. Moving first in the district court for a stay would thus be impracticable.

CONCLUSION

For the foregoing reasons, Kaspersky Lab respectfully requests that the Court stay implementation of Sections 1634(a) and (b) of the NDAA, the interim rule, and any implementing regulations before July 16, 2018, and until this Court

resolves the Bill of Attainder Case on the merits. In the event the Court declines to grant emergency relief before July 16, 2018, Kaspersky Lab requests that this Court consider this motion for a stay at oral argument on September 14, 2018.

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. 27(d), the foregoing Emergency Motion is proportionately spaced, has a typeface of 14-point or more, and contains 5,190 words.

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 with the Clerk of the Court for the United States Court of Appeals for the District of Columbia Circuit by using the CM/ECF system. Participants in the case who are registered CM/ECF users will be served by the CM/ECF system. I also certify that I have caused four copies of the foregoing to be hand delivered to the Court. I also certify that I have caused the foregoing to be electronically mailed to:

Lewis S. Yelin
Senior Counsel
H. Thomas Byron III
Assistant Director
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
Lewis.Yelin@usdoj.gov
H.Thomas.Byron@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

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

KASPERSKY LAB, INC. and KASPERSKY LABS LIMITED Plaintiffs, v. U.S. DEPARTMENT OF HOMELAND SECURITY and KIRSTJEN NIELSEN, in her official capacity as Secretary of Homeland Security Defendants.	Civ. Act. No. 17-cv-02697-CKK

ANGELO GENTILE'S DECLARATION IN SUPPORT OF PLAINTIFFS' MOTION FOR SUMMARY JUDGMENT

I, Angelo Gentile, hereby declare:

1. I make this Declaration in support of Plaintiffs' Motion for Summary Judgement, in the above captioned case.

2. This Declaration is based on my personal knowledge of the matters stated herein.

3. Since August 2016, I have held the title of Executive Vice President, Finance and Operations of Plaintiff Kaspersky Lab, Inc.

4. Kaspersky Lab, Inc. is a Massachusetts corporation, based in Woburn, Massachusetts, and is a direct wholly-owned subsidiary of its U.K. parent, Kaspersky Labs Limited, the ultimate holding company for all Kaspersky Lab group entities (hereinafter,

Plaintiffs Kaspersky Lab, Inc. and Kaspersky Labs Limited collectively "Kaspersky Lab" or the "Company"). Kaspersky Lab, Inc. serves as the North American headquarters of Kaspersky Lab.

5. In my capacity as Executive Vice President, Finance and Operations of Kaspersky Lab, Inc., I oversee the operations and financial management—i.e., financial planning, performance, and reporting—of the company, including for the company's revenue from sales through channel partners to consumers as well as commercial and government customers in the U.S. and Canada.

6. Prior to this role, I served as Senior Vice President, Finance and Administration of Kaspersky Lab, Inc. from November 2004 to August 2016, at which time I was responsible for the strategic financial management of Kaspersky Lab's North American sales and operations.

7. I have been continuously employed by Kaspersky Lab, Inc. ever since the company's incorporation in 2004.

8. I have more than three decades of financial management experience at technology companies. I graduated from Northeastern University in 1984 with a Bachelor of Science in Finance and Accounting. Prior to joining Kaspersky Lab, Inc., I served as Vice President, Finance at Riverdeep Group, plc. Prior to Riverdeep, I was Chief Financial Officer at Invention Machine Corporation and Chief Financial Officer at USTeleCenters.

KASPERSKY LAB

9. Kaspersky Lab is a multinational cybersecurity company focused exclusively on protecting its customers against cyberthreats, no matter their origin. It is one of the world's largest privately owned cybersecurity companies, operating in nearly 200 countries and territories and maintaining 35 offices in 31 countries. Among its offices are research and development centers employing anti-malware experts in the U.S., Europe, Japan, Israel, China,

Russia, and Latin America. Over 400 million users—from governments to private individuals, commercial enterprise to critical infrastructure owners and operators alike—utilize Kaspersky Lab technologies to secure their data and systems. Kaspersky Lab consistently ranks among the world's top four vendors of security solutions for endpoint users.

10. Kaspersky Lab products routinely score the highest ratings in a broad spectrum of independent tests and reviews. In 2017, Kaspersky Lab participated in more independent tests and reviews than any other cybersecurity vendor—86 tests in total, whereas the closest competitor participated in only 68 tests. Kaspersky Lab products outperformed all other cybersecurity vendors in independent tests, receiving 72 first place finishes. The Company's products were also ranked among the top three products in 78 of the 86 tests, i.e., in 91% of all product tests in 2017, with its closest competitor achieving a top-three finish in only 72% of tests.

11. Kaspersky Lab was founded in 1997 by Eugene Kaspersky and a small group of associates. Mr. Kaspersky has been the CEO of Kaspersky Lab since 2007. Although the Company's global headquarters are in Moscow, more than 80% of its sales are generated outside of Russia. Kaspersky Lab's presence in Russia and its deployment in areas of the world, in which many sophisticated cyberthreats originate, situates the Company to be a unique and essential partner in the fight against such threats, which, in its absence, may not otherwise be met.

12. Consistent with the practice of most multinational software companies, Kaspersky Lab operates a two-tier channel sales model, by which it sells Kaspersky Lab products to end users through distributors and resellers. Therefore, the Company relies on the sales channel, particularly on its reseller partners, to identify and pursue sales leads in both the private and public sector, and works to enable its partners to realize each and every sales opportunity, regardless of its target.

KASPERSKY LAB, INC. AND ITS U.S. BUSINESS

13. The U.S. has historically been one of the most significant geographic markets in Kaspersky Lab's global business. Sales to customers in the U.S. represented approximately one quarter of total global bookings in 2016.

14. Kaspersky Lab, Inc. has invested over half a billion dollars in the U.S. over the last thirteen years, and over $60 million in 2017 alone.

15. A fraction of Kaspersky Lab, Inc.'s U.S. sales, driven by (independent) resellers in the sales channel, has been to the U.S. government. Active licenses held by federal agencies in September 2017 had a total value (to Kaspersky Lab, Inc. and the Company as a whole) of less than $54,000—approximately 0.03% of Kaspersky Lab, Inc.'s annual U.S. sales at the time.

16. It is not possible for Kaspersky Lab, Inc. to assess which and what portion of its former, current or prospective customers were, are currently, or may be prospective U.S. federal government contractors. Such customer characteristics are not recorded in our sales systems.

REPUTATIONAL HARM CAUSED BY BOD-17-01

17. In my roles for Kaspersky Lab, Inc., I am responsible for reporting the financial results for our North American operations to Kaspersky Labs Limited in the U.K., where the Company's accounts are audited by KPMG and filed with the U.K. Companies House.[1] I work closely with my colleagues in London and Moscow who are responsible for the Company's accounts, including to assess the impact of Kaspersky Lab, Inc.'s performance on the Company's operations and the accounts of Kaspersky Labs Limited. This specifically has included assessing the impact of Binding Operational Directive 17-01 (the "BOD") which the U.S. Department of Homeland Security (DHS) issued on September 13, 2017. The BOD (as accompanied by DHS's

[1] *See* https://beta.companieshouse.gov.uk/company/04249748/filing-history

press release[2]) branded our antivirus software products and services "information security risks" to U.S. government information systems, and summarily ordered their removal and permanent debarment from those systems.

18. Kaspersky Lab has a substantial interest in the continued ability for its resellers to sell its products to the U.S. government and federal contractors, although, historically, only a small fraction of Kaspersky Lab, Inc. sales (through resellers) have been made to the U.S. government itself, as explained above. In addition to the Company's direct loss of both federal government and federal contractor customers, subject to the BOD prohibition, DHS's labeling Kaspersky Lab's antivirus software products "information security risks" and summarily banning them from all government agencies has had, and continues to have, a profound impact on the Company's brand, reputation, and prospects everywhere that it does business. The BOD has affected the use of those same products by our commercial customers and individual consumers and the reputation that our products enjoyed with those (current and potential) users.

19. For example, several substantial tenders for the provision of Kaspersky Lab products, which were in process at the time of the BOD, were terminated by customers as a result of its issuance. In these cases, the prospective customers have often reiterated their belief that Kaspersky Lab offered the best technical solution for their needs, but that they were unwilling or unable to proceed with the purchase due to DHS's action.

20. Even where our partners have been successful in making sales of Kaspersky Lab products, we have been receiving and processing an unprecedented volume of product return and early termination requests since the issuance of the BOD. Many customers returning or

[2] See U.S. Department of Homeland Security, DHS Statement on the Issuance of Binding Operational Directive 17-01, Sept. 13, 2017, https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01

terminating Kaspersky Lab software licenses for a refund specifically cite the BOD and the language used to support it as the reason for making the return. These concerns are difficult for the Company to address so long as the BOD remains in effect. Kaspersky Lab's position as a trusted software vendor has been compromised in all areas, which has resulted in the Company accepting returns that would have otherwise been rejected under our standard returns policy.

21. Existing and prospective Kaspersky Lab customers have referred to, and continue to refer to, the BOD (most often, referring to it as the "DHS ban" or the "Homeland Security ban") in a variety of scenarios, all of which contribute to the adverse financial and reputational impact of the BOD on Kaspersky Lab.

a. Existing Kaspersky Lab customers have referred to the BOD when:

   i. making returns or otherwise prematurely terminating subscriptions for licenses for Kaspersky Lab software or services and demanding refunds for the same, with the BOD being the sole reason for such return or termination; and

   ii. deciding not to renew their Kaspersky Lab software license, even though the customer was otherwise satisfied with the product's performance after prolonged use, with the BOD being the sole reason for choosing not to renew.

b. Prospective Kaspersky Lab customers have referred to the BOD when ultimately deciding to purchase competitor products rather than Kaspersky Lab's even where, per the customer's explanation, Kaspersky Lab's solution had prevailed as the most suitable technical solution in the tender process.

22. These customers, which specifically refer to the BOD in the circumstances described above, include Fortune 500 companies, small businesses, state and local government agencies, public and private educational institutions, and consumers.

23. Many of the Company's corporate customers turned out to be federal contractors or to be bidding on federal contracts at the time of the BOD. In making returns or not renewing their licenses, these customers referred to the BOD's direct implications on their software security choices, i.e., the express prohibition of the use of Kaspersky Lab products for federal contractors operating within federal information systems.

24. Though the loss of the federal contractor customers was significant, the majority of the Company's losses attributable to the BOD has been due to its resulting reputational damage to and loss of trust in Kaspersky Lab products in the U.S. market. Our sales teams have reported customers referring to the BOD as the primary reason for their decisions not to use Kaspersky Lab solutions as early as the day the BOD was announced on September 13, 2017 and continuing into 2018 through the present date.

ADVERSE FINANCIAL IMPACT OF BOD-17-01

25. Due to the effective debarment resulting from the BOD, Kaspersky Lab immediately lost revenue that may have been generated by license renewals by existing federal government customers and new sales to federal government customers. Furthermore, Kaspersky Lab lost revenue that would have been generated by license renewals by existing customers and new sales to customers that were either federal contractors or who may wish to bid on federal contracts in the future. Moreover, the BOD's damage to Kaspersky Lab's reputation has severely impacted Kaspersky Lab's U.S. commercial and consumer sales. This impact is continuing and growing. Kaspersky Lab books for Fiscal Year 2017 were closed on January 17,

2018. Much of the 2017 data in this Declaration is taken from these results. Kaspersky Lab's sales results for the month of January 2018, also referred to in this Declaration, were finalized on February 7, 2018.

26. Several U.S. retailers have removed Kaspersky Lab products from their shelves and online stores and suspended their long-standing partnerships with Kaspersky Lab after the issuance of the BOD. Some of these retailers, which provided a steady stream of both new customers and consumer product subscription renewals to Kaspersky Lab over the years, went even further and encouraged and otherwise incentivized existing Kaspersky Lab software customers (current license holders) to "switch" to the software of one of our competitors. As a result of these actions, Kaspersky Lab Inc.'s 2017 Q3 gross bookings from retail sales in the U.S. immediately fell 37% compared to the same period in 2016.

27. The first full quarter immediately following the issuance of the BOD showed an even steeper decline. Kaspersky Lab, Inc.'s gross bookings from U.S. retail sales in 2017 Q4 fell 61% compared to the same period in 2016. The Company's gross bookings from U.S. retail sales in the second half of 2017 were 50% lower than they were during the same period in 2016.

28. The Company's net U.S. retail bookings in January 2018 were down 107% from the same period last year. The decline of more than one hundred percent means the Company not only lost virtually all retail bookings from the termination of major retail partnerships but also remains obligated to issue refunds on customer returns of retail products and pay additional operational costs connected with such returns. Therefore, the Company has recently been incurring a negative revenue amount in the retail sector on a monthly basis.

29. Kaspersky Lab, Inc.'s net loss from product returns and early terminations by U.S. customers from September through December 2017 totalled $237,312.73. By contrast, net loss from product returns during the same period last year totalled only $10,033.16.

30. In addition to these losses in the consumer market, the BOD has also caused significant damage to Kaspersky Lab, Inc.'s business-to-business ("B2B") segment. The Company's B2B business includes sales to traditional private sector corporate customers, some of which may have been (or been hoping to become) federal contractors when the BOD was issued, as well as non-federal government public sector customers from state and local government agencies and educational institutions ("SLED").

31. The Company's 2017 bookings from B2B sales fell 33% in Q3 and 45% in Q4 when compared to the same period in 2016. B2B bookings from U.S. customers in the month of January 2018 have declined 46% compared to the same period in 2017. The B2B renewal rate has gone down 36 percentage points to only 26% of existing corporate customers renewing in January 2018 from 62% of such customers renewing in the same period last year.

32. The significant decline in the Company's B2B segment, resulting from both the decline in corporate customer retention and the decline in new corporate customer acquisition, can be, at least in part, specifically attributed to the BOD. Shortly after the issuance of the BOD, Kaspersky Lab learned that many of its B2B customers were, in fact, federal contractors and, thus, subject to the BOD's prohibition of Kaspersky Lab software. None of these customers waited until DHS's Final Decision on the BOD, expected in December 2017, before informing the Company's reseller partners of their intention to terminate their Kaspersky Lab subscriptions and demanding refunds for their terminated subscriptions.

33. There have been several instances of technical stakeholders of enterprise customers, following prolonged use or testing of Kaspersky Lab products, choosing to move forward with Kaspersky Lab solutions as the best software security option for their enterprise's needs, but, when seeking requisite purchase approvals from business stakeholders within their organization, i.e., C-suite executives and/or the Board of Directors, such technical stakeholders were met with resistance or outright rejection by those business stakeholders due to the significant reputational harm caused by the BOD. Such business stakeholders have specifically referred to the BOD and the language used to support it as the primary reason for ultimately rejecting Kaspersky Lab solutions for their organizations and additionally cited concerns that the use Kaspersky Lab solutions could cause damage to their own organizations' reputations following the BOD.

34. Since Kaspersky Lab operates under a two-tier channel sales model, the Company relies on the channel, particularly its reseller partners, to identify and pursue sales leads in both the private and public sectors. Several key reseller partners expressed that they have lost confidence in the Kaspersky Lab brand due to the BOD. As a result, many of these partners significantly decreased activity in pursuit of net new business opportunities on behalf of Kaspersky Lab, opting to promote our competitors' solutions as the "easier sell" in the current climate. Several key reseller partners have removed Kaspersky Lab products from their published product lists or ceased quoting Kaspersky Lab products to customers altogether, specifically referring to the DHS action as the reason for doing so. Such reactions to the BOD by many reseller partners have significantly diminished Kaspersky Lab's pipeline of sales opportunities and continue to impair the Company's ability to compete with other cybersecurity software vendors in the U.S. market. Sales through the Company's historically highest

performing reseller partners have gone down 40-60% compared to the same period the year before in every calendar month since the issuance of the BOD through the present date.

35. In addition to damaging our relationship with our reseller partners, the BOD has also adversely affected the Company's own ability to reach new customers and increase brand awareness. Several broadcast and print media outlets, which aired or placed Kaspersky Lab ads over the course of several years prior to the issuance of the BOD, refused to air or place further Kaspersky Lab advertising in the course of one month following the issuance of the BOD.

36. The BOD has caused further collateral harm to Kaspersky Lab's business with State and municipal government agencies. Prior the BOD, Kaspersky Lab had a significant number of state and local government customers and education sector customers (collectively "SLED Customers"). For example, in August 2017, one of the Company's SLED Customers, a municipality in Illinois, renewed its Kaspersky Lab software license. Just two business days after the BOD issuance, this customer terminated the just-renewed Kaspersky Lab software license and demanded a refund for the same. When asked the reason for seeking early termination and the refund, the customer replied by simply copying and pasting the first two paragraphs of the DHS press release on the BOD[3] and further stating that it intends to use the refunded amount to purchase a non-Kaspersky Lab solution.

37. On the same day that the BOD was issued, the Multi-State Information Sharing & Analysis Center ("MS-ISAC") sent a mass email addressed to all of its intelligence partners and members, many of which were Kaspersky Lab SLED Customers at the time, containing an advisory alert titled "Cyber Alert: DHS Issues Binding Operational Directive on Kaspersky

[3] *See infra* note 2.

Products"[4] (the "MS-ISAC Alert"). The MS-ISAC Alert contained a summary of the BOD, a link to the DHS Statement on the BOD, and the following recommendation to its members: "The MS-ISAC recommends members follow the guidance in the federal directive." Kaspersky Lab learned of the MS-ISAC Alert when one of its SLED Customers, a municipality in Nevada, forwarded it to the Company's reseller partner to explain why the customer had decided not to renew its large-value Kaspersky Lab software license just three business days after the BOD.

38. The BOD also induced a number of States to follow suit in issuing analogous directives, which expressly prohibit (or strongly recommend against) the use of Kaspersky Lab products by subject State and municipal government agencies (the "State Directives"). Some of these State Directives are specifically based on, and exclusively refer to, the BOD as their justification. In fact, such State Directives simply repeat the language DHS used in support of the BOD. Due to the State Directives, many of the Company's SLED Customers were required or otherwise strongly pressured to discontinue their use of Kaspersky Lab software and solutions.

39. The first instance of such a State Directive, which specifically refers to the BOD, appeared only two days after the BOD in New York State. On September 15, 2017, the New York Office of General Services issued General Information Bulletin CL # 843[5] (the "New York Directive"), the purpose of which, per the opening sentence, is to "advise authorized users of centralized information technology contracts established by the New York State Office of General Services ("OGS") of data privacy and security concerns related to products sold by

[4] *See* Center for Internet Security, Multi-State Information Sharing & Analysis Center, *Cyber Alert: DHS Issues Operational Directive on Kaspersky Products*, Sept. 13, 2017, https://www.cisecurity.org/ms-isac/dhs-issues-binding-operational-directive-on-kaspersky-products/

[5] *See* New York State Office of General Services, *General Information Bulletin*, CL #843 *Subject: Kaspersky Lab Software and Cybersecurity Services,* Sept. 15, 2017, https://www.ogs.ny.gov/purchase/spg/pdfdocs/CL843.pdf

Kaspersky Lab." The next sentence of the New York Directive reads "On September 13, 2017, the U.S. Department of Homeland Security ("DHS") directed federal agencies to identify, remove, and discontinue current and future use of products manufactured by Kaspersky Lab, a Russian cybersecurity and software company that DHS characterized as possibly vulnerable to Russian government influence...." The New York Directive concludes with recommendations that New York State departments contact their IT departments "to commence a review of purchases and contracts for software and services to determine their exposure to Kaspersky Lab products and services." Kaspersky Lab has lost several high-value license renewals and new license deals with New York State customers as a direct result of the New York Directive.

40. The second instance of such State Directives that specifically refers to the BOD appeared in Texas. On October 30, 2017, the Texas Education Agency issued a Cyber Alert titled "DHS Issues Binding Operational Directive on Kaspersky Products"[6] (the "Texas Directive"), which contains a summary of the BOD and follows with two recommendations. The Texas Directive concludes by recommending that, in light of the high volume of sensitive student information collected, Education Service Centers and Local Educational Agencies in Texas "follow the guidance in the federal directive." Immediately following the Texas Directive, several existing customers from the education sector in Texas informed the Company's reseller partner that the Education Service Centers were directing school boards to remove Kaspersky Lab software from their machines and networks. As a result, affected customers demanded refunds for the Kaspersky Lab software licenses they were prohibited from using.

---

[6] *See* Texas Education Agency, *Cyber Alert: DHS Issues Binding Operational Directive on Kaspersky Products,* Oct. 30, 2017, https://tea.texas.gov/About_TEA/News_and_Multimedia/Correspondence/TAA_Letters/Cyber_Alert__DHS_Issues_Binding_Operational_Directive_on_Kaspersky_Products/

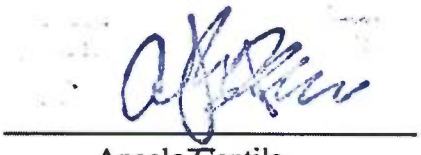
41. All of the above has, in turn, reduced Kaspersky Labs Limited's return on its investment in Kaspersky Lab, Inc., and has lowered the value of its shareholdings in that subsidiary. While sales to customers in the U.S. represented approximately one quarter of total global bookings in 2016, the U.S. accounted for only one fifth of total global bookings in 2017.

42. The damage to Kaspersky Lab caused by the BOD is not limited to the Company's sales performance in the United States. Colleagues from around the world, including in Latin America, Europe, and Asia, have reported on premature terminations and lost deals, in which the existing or prospective customer specifically refers to the BOD and the labeling of Kaspersky Lab products as an "information security risk" for the U.S. Government as the reason for terminating or not closing a deal for Kaspersky Lab software and services.

43. Kaspersky Lab, Inc. has also seen a substantial headcount reduction from 281 employees in the U.S. on September 12, 2017 (the day before the BOD was issued) to 253 U.S. employees at the end of January 2018, representing a 10% reduction in headcount. This decline is largely attributable to: i) voluntary departures from the Company caused by a fall in staff morale due to the attacks on the reputation and integrity of the Company and its products (including through the BOD and statements made by DHS officials); and ii) layoffs necessitated by falling revenues. Most recently, in January 2018, we were forced to lay-off 24 employees in the course of two weeks.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on February 22, 2018.



Angelo Gentile

UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

KASPERSKY LAB, INC. and KASPERSKY LABS LIMITED, 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, Appellees.	Case Nos. 18-5176 & 18-5177

SUPPLEMENTAL DECLARATION OF ANGELO GENTILE

I, Angelo Gentile, hereby declare:

1. I am the Executive Vice President, Finance and Operations of Kaspersky Lab, Inc. In that capacity, I oversee the operations and financial management—i.e., financial planning, performance, and reporting of the company, including for the company's revenue from sales through channel partners to consumers as well as commercial and government customers in the United States and Canada. This declaration supplements my declaration dated February 22, 2018 that was submitted to the District Court. I have personal knowledge of the information contained in this declaration and, if called as a witness, could and

would competently testify thereto.

2. Section 1634(a) of the National Defense Authorization Act for Fiscal Year 2018 (the "NDAA") has caused harm to Kaspersky Lab separate from and in addition to the harm caused by the Binding Operational Directive 17–01 ("BOD"). The BOD states that it "does not address the following Kaspersky services: Kaspersky Threat Intelligence and Kaspersky Security Training." Binding Operational Directive BOD-17-01, p. 2 (Sept. 13, 2017). Those threat intelligence and security training services are prohibited under Section 1634(a)'s ban on "services developed or provided" by Kaspersky Lab and its affiliates.

3. Kaspersky Lab provides a Threat Intelligence Portal to help businesses access the most relevant threat information and augment their efforts to mitigate complex cyberthreats. The Threat Intelligence Portal provides subscribers with a single point of access to specific services provided by Kaspersky Lab, including Threat Data Feeds, Custom Intelligence Reporting, APT Intelligence Reporting and Threat Lookup Service. Subscribers have on-demand access to both the latest and historical threat intelligence to prevent or detect cyberattacks before they affect their organization. This access improves awareness of modern tools and techniques used by dangerous threat actors and thereby improves the organization's detection times, incident response times, and forensic capabilities to limit the impact of advanced threats.

4. Kaspersky Lab also provides Security Training services that combine industry best practices with real-life field experience, applying proven learning techniques to address all levels of an organization's structure. The Security Training services include security training for information technology ("IT") professionals, security awareness for non-IT professionals, Kaspersky Interactive Protection Simulation, Cybersafety Management Games, and Employment Skills Training Program. Each security training emphasizes the personal importance of cybersecurity, as more than 80% of all enterprise cyber-incidents are caused by employee error and negligence. Kaspersky Lab's security training emulates the employee's workplace and behavior, drawing users' attention to their practical interests, thus contributing to the motivation to learn and increasing the likelihood that the skills will be applied.

5. Agencies of the federal government and government contractors that have used our threat intelligence and security training services are prohibited from using these services under Section 1634(a) of the NDAA. In addition to damaging our relationship with agency and contractor clients, Section 1634(a) has adversely affected Kaspersky Lab's reputation, not only compromising customer trust of the company's security software but also of its non-software services such as threat intelligence and security trainings. This reputational harm has adversely impacted

Kaspersky Lab's ability to not only maintain its customer base but also reach new customers and increase brand awareness.

I declare under penalty of perjury that the foregoing is true and correct.

Executed at Woburn, Massachusetts on June 27, 2018.

Angelo Gentile

UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

KASPERSKY LAB, INC. and KASPERSKY LABS LIMITED, 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, Appellees.	Case Nos. 18-5176 & 18-5177

DECLARATION OF BRETT MATESEN

I, Brett Matesen, hereby declare:

1. I am the Director of Business Development for Kaspersky Lab, Inc. and have served in that position since January 2009. I report to the Head of Technology Licensing and am responsible for managing Kaspersky Lab's relationship with independent software vendors in the Americas. In particular, I help to sell Kaspersky Lab technology, including embedded code, to technology vendors. I have personal knowledge of the information contained in this declaration and, if called as a witness, could and would competently testify thereto.

2. Kaspersky Lab has been a leading contributor to the information security community for more than 20 years. Kaspersky Lab's work in various regions of the world where many sophisticated cyberthreats originate makes it a unique and essential partner in the fight against such threats.

3. Section 1634(a) of the National Defense Authorization Act for Fiscal Year 2018 (the "NDAA") has caused harm to Kaspersky Lab that is separate from and in addition to the harm caused by the Binding Operational Directive 17–01 ("BOD"). Section 1634(a) has caused harm to Kaspersky Lab's technology alliance partnerships because of the ban on using Kaspersky Lab's embedded code resulting from the prohibition on using "any . . . software, or services developed or provided, in whole or in part, by . . . Kaspersky Lab" and its affiliates. The BOD, by contrast, states that it "does not address Kaspersky code embedded in the products of other companies." Binding Operational Directive BOD-17-01, p. 2 (Sept. 13, 2017).

4. Technology vendors license a variety of Kaspersky Lab technology, including our malware databases, our scan and detection engine, and other security technologies, including code embedded in other companies' products.

5. Section 1634(a)'s prohibition on using Kaspersky Lab's embedded code has a substantial effect on government contractors. For example, the University of California system, which is a large federal contractor, ordered all

U.C. campuses not to buy or deploy Kaspersky Lab products, citing as an example technology that uses "embedded Kaspersky code." "UC Orders Moratorium on New Purchases or Uses of Kaspersky Lab Products" (Dec. 8, 2017) (https://iet.ucdavis.edu/content/uc-orders-moratorium-new-purchases-or-uses-kaspersky-lab-products).

6. Kaspersky Lab had several high-profile technology partners (outbound license customers) who are federal contractors. Agreements for outbound licensing of Kaspersky Lab technology traditionally renew automatically over different agreed upon terms until one of the parties takes steps to terminate the agreement.

7. A significant number of Kaspersky Lab's technology partners have terminated their relationships, citing concerns about Section 1634(a)'s prohibition on using Kaspersky Lab embedded code in technology products for federal government customers. These relationships provided Kaspersky Lab with several million dollars in revenue annually and would have continued through and after October 1, 2018 but for Section 1634(a). As a result, Kaspersky Lab has lost significant income, totaling millions of dollars, that it otherwise would have received from the partnerships in place prior to Section 1634(a), some of which spanned many years.

8. In addition to damaging our existing relationships with technology and software vendors, Section 1634(a) has adversely affected Kaspersky Lab's reputation and the ability to reach new customers and increase brand awareness. Potential new vendors for using Kaspersky Lab embedded code have withdrawn their interest, citing concerns about Section 1634(a) of the NDAA.

I declare under penalty of perjury that the foregoing is true and correct. Executed at Seattle, Washington on June 27, 2018.

Brett Matesen