[ORAL ARGUMENT SCHEDULED FOR SEPT. 14, 2018]

No. 18-5176
(consol. No. 18-5177)

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

KASPERSKY LAB, INC., and KASPERSKY LABS LIMITED,

Plaintiffs-Appellants,

v.

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

Defendants-Appellees.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

BRIEF FOR APPELLEES

CHAD A. READLER
Acting Assistant Attorney General

H. THOMAS BYRON III
LEWIS S. YELIN
Attorneys, Appellate Staff
Civil Division, Room 7239
U.S. Department of Justice
950 Pennsylvania Ave., NW
Washington, DC 20530
(202) 514-3425

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

Pursuant to D.C. Circuit Rule 28(a)(1), the undersigned counsel certifies as follows:

A. Parties and Amici.

Kaspersky Lab, Inc., and Kaspersky Labs Ltd. were plaintiffs in the district court in Nos. 17-2697 and 18-325 and are appellants in this Court in Nos. 18-5176 and 18-5177. The United States Department of Homeland Security and Kirstjen M. Nielsen, in her official capacity as Secretary of Homeland Security, were defendants in the district court in No. 17-2697 and appellees in this Court in No. 18-5176. The United States of America was defendant in the district court in No. 18-325 and is appellee in this Court in No. 18-5177.

B. Rulings Under Review.

The ruling under review is a final order of the district court, *Kaspersky Lab, Inc. v. United States Department of Homeland Security*, which is reported at 2018 WL 2433583 (May 30, 2018), and reproduced in the Joint Appendix at 169-223.

C. Related Cases.

I am aware of no related case pending in this or any other court.

s/ Lewis S. Yelin
LEWIS S. YELIN
Counsel for Appellees

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page:

Cases

Statutes

Rules

Regulations

Legislative Materials

Administrative Material

Other Authorities

GLOSSARY

BOD-17-01	Binding Operational Directive BOD-17-01 (Sept. 13, 2017)
FSB	Russian Federal Security Service
NDAA	National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, 131 Stat. 1283, 1739 (2017)

STATEMENT OF JURISDICTION

The district court entered final judgment on May 30, 2018. Plaintiffs filed their notice of appeal on June 6, 2018, which is timely under Federal Rule of Appellate Procedure 4(a)(1)(B). This Court has jurisdiction under 28 U.S.C. § 1291.

STATEMENT OF THE ISSUES

1. Whether the district court correctly held that Section 1634 of the National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, 131 Stat. 1283, 1739 (2017) (NDAA § 1634), Add. 1, is not a bill of attainder;

2. Whether the district court correctly held that it lacks jurisdiction to consider plaintiffs' challenge to Binding Operational Directive BOD-17-01, 82 Fed. Reg. 43,782 (Sept. 19, 2017) (BOD-17-01 or directive), Add. 4, because a favorable decision would not redress their alleged injuries in light of NDAA Section 1634.

PERTINENT STATUTE AND ADMINISTRATIVE ORDER

Section 1634 of the NDAA and the directive are reprinted in an addendum to this brief. The pre-publication version of the directive also appears at JA 53-55.

STATEMENT OF THE CASE

I. NATURE OF THE CASE

These consolidated appeals arise from two related cases challenging distinct government actions. Plaintiffs Kaspersky Lab, Inc., and Kaspersky Labs Limited

(Kaspersky) first brought suit to challenge a binding operational directive, an administrative action issued by the Department of Homeland Security (DHS). JA 1-22. The directive set out a timeline for federal agencies to identify Kaspersky-branded products on federal information systems, develop a plan to remove such products, and, unless directed otherwise by DHS, begin removing the products. 82 Fed. Reg. at 43,783; Add. 5. Kaspersky challenged the directive under 5 U.S.C. § 706(2)(B) of the Administrative Procedure Act (APA), alleging that the BOD was issued in violation of Kaspersky's procedural due-process rights. JA 21. Kaspersky also claimed that DHS's issuance of the directive was unsupported by substantial evidence and should be set aside under 5 U.S.C. § 706(2)(A). JA 21-22. Kaspersky sought an order invalidating the directive and a declaration that Kaspersky-branded products on federal information systems "do not present a known or reasonably suspected information security threat, vulnerability, and risk to federal information systems." JA 22.

Kaspersky filed a second suit challenging NDAA Section 1634 as an unconstitutional bill of attainder. JA 149-50. Section 1634(a) prohibits any federal government entity from using "any hardware, software, or services developed or provided, in whole or in part," by Kaspersky or entities controlled by Kaspersky. Add. 1. That prohibition becomes effective October 1, 2018. NDAA § 1634(b);

Add. 2. Kaspersky sought a declaration that Sections 1634(a) and (b) are unconstitutional and an order invalidating those provisions. JA 150.

II. ADMINISTRATIVE BACKGROUND

The United States government's networks and computers are a strategic national asset, and their security depends on the government's ability to act swiftly and effectively in the face of rapidly evolving cyberthreats. To protect that critical asset, Congress vested the DHS Secretary with broad discretion to take appropriate action to protect federal information systems against cyberintrusions. One tool Congress gave the Secretary is the authority to issue binding operational directives, identifying compulsory actions federal agencies must take in response to a "known or reasonably suspected information security threat, vulnerability, or risk." 44 U.S.C. § 3552(b)(1)(A); see *id.* § 3553(b)(2). The Secretary exercises that authority in reliance on expert predictive judgments, often based on sensitive or classified intelligence reporting, about whether a particular threat or vulnerability is serious enough to warrant a government-wide response. See, *e.g.*, JA 29-46 (Memorandum from Jeanette Manfra, Assistant Sec'y for Cybersecurity & Cmmc'ns, Nat. Prot. & Programs Directorate, DHS to the Acting Sec'y 2 (Sept. 1, 2017) (First Manfra

Mem.)); JA 31 (referencing annex containing classified material relevant to BOD-17-01).[1]

A. Issuance of the Directive

Based on extensive investigation and consultation with cybersecurity experts, the DHS Acting Secretary determined that the Russian government, on its own or in collaboration with Kaspersky, could use Kaspersky-branded software and services as an entry point for espionage or other hostile cyberactivities against federal information and information systems. JA 48-52 (Decision, Memorandum of the Acting Secretary, Binding Operational Directive 17-01 (Sept. 13, 2017) (Decision of the Acting Sec'y). In light of that determination, on September 13, 2017, the Acting Secretary issued the directive, requiring federal agencies to identify Kaspersky-branded products on federal information systems within thirty days of the issuance of the directive, develop a plan within sixty days for the removal of such products, and, ninety days after issuance of the directive, begin implementation of the plan,

[1] Although the Acting Secretary was presented with classified information to inform her decision whether to issue the directive, the Acting Secretary determined that the directive is justified on the strength of the unclassified evidence alone. JA 51.

unless DHS otherwise directs based on its consideration of new information.[2] 82 Fed. Reg. at 43,783, Add. 5; see *id.* (defining "Kaspersky-branded products").

The Acting Secretary's action was based on the following considerations. First, all antivirus software "operates with broad file access and elevated privileges." JA 30 (First Manfra Mem.); see JA 33-35. Such deep integration into operating systems "can be exploited by a malicious cyber actor such as Russia, which has demonstrated the intent to target the U.S. government" and has the "capability to exploit vulnerabilities in federal information systems." JA 30; see JA 35-37.

Second, DHS concluded that Kaspersky has a particular relationship with the Russian Federation that makes it a specific threat to federal information systems. Russian law authorizes the Russian Federal Security Service (FSB) "to compel Russian enterprises to assist the FSB in the execution of FSB duties, to second FSB agents to Russian enterprises (with the enterprise's consent), and to require Russian companies to include hardware or software needed by the FSB to engage in 'operational/technical measures.'" JA 30; see JA 40-41. In addition, Kaspersky "relies on the FSB for needed business licenses and certificates," which the FSB

[2] Due to statutory limitations, the directive does not cover national security systems and certain other systems operated by the Department of Defense and the intelligence community. See 44 U.S.C. § 3553(b), (d) & (e); JA 48 n.1 (Decision of the Acting Sec'y).

could condition on Kaspersky's cooperation. JA 30; see JA 41-42. Further, "Russian law allows the FSB to intercept all communications transiting Russian telecommunication and Internet Service Provider networks," which DHS presumed, and Kaspersky did not dispute, "includes data transmissions between Kaspersky and its U.S. government customers." JA 30. And Kaspersky officials have "personal and professional ties to Russian government agencies," such as Russian intelligence agencies. JA 38; see JA 38-39, 42; see also JA 68-69 (Memorandum from Jeanette Manfra, Assistant Sec'y for Cybersecurity & Commc'ns, Nat. Prot. & Programs Directorate, DHS to the Acting Sec'y, at 13-14 (Dec. 4, 2017) (Second Manfra Mem.)) (further detailing ties between Kaspersky officials and the Russian government). Moreover, House and Senate committees held hearings earlier in 2017 to gather information about the risk of Kaspersky software on federal information systems, including a hearing at which the heads of six United States intelligence agencies testified about concerns related to Kaspersky software. JA 42-43.

The Acting Secretary's decision to issue the directive was based on those concerns. See JA 49-50 (Evidence and Analysis).

B. Administrative Process

On the day DHS issued the directive, the agency sent Kaspersky a letter (see JA 58), enclosing the Secretary's decision memorandum (see JA 48-52) and

explaining the administrative process providing "entities whose commercial interests are directly impacted by BOD 17-01 the opportunity to respond" and seek DHS's review of the directive (82 Fed. Reg. at 43,784; Add. 6). Under that process, Kaspersky or any other commercially affected entity could initiate a review of the directive by submitting, by November 3, 2017, "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." 82 Fed. Reg. at 43,784; Add. 6; see 82 Fed. Reg. at 43,783; Add. 5 (directing agencies to begin removal of Kaspersky-branded products ninety days after September 13, 2017, "unless directed otherwise by DHS based on new information"). Upon the receipt of such a response, a senior DHS official would review the material and make a recommendation to the Secretary, who would then make a final decision. 82 Fed. Reg. at 43,784; Add. 6.

On September 29, 2017, DHS sent Kaspersky's counsel the First Manfra Memorandum, with exhibits, at counsel's request, "to ensure that Kaspersky had the complete unclassified rationale for issuance of [the directive]." JA 58. Kaspersky subsequently submitted a response to DHS, along with seven exhibits. See JA 56 & n.1. The Kaspersky submission included a technical assessment from Kaspersky's expert, JA 62-64; the comments of Kaspersky's expert concerning the risk posed by other antivirus software, JA 74-77; Kaspersky's proposed risk mitigation, JA 64-68;

Kaspersky's comments regarding its ties to the Russian government, JA 68-69; its response to DHS's assessment of the risks posed by Russian law, JA 69-71; Kaspersky's comments concerning the FSB's control over its licenses and certificates, JA 71-72; Kaspersky's response to concerns raised by federal officials, including the heads of U.S. intelligence agencies, JA 72-73; and Kaspersky's legal arguments, JA 78-79. DHS also "met with two Kaspersky U.S. officials and their counsel" on November 29, 2017, to discuss Kaspersky's submission "and related topics." JA 59.

DHS considered "the totality of the administrative record," including Kaspersky's lengthy submission; the information the directive required federal agencies to submit, JA 59-60; an analysis of applicable Russian law prepared by Professor Peter Maggs of the University of Illinois College of Law, JA 60, 69-71, see JA 81-125; and a supplemental information security-risk assessment prepared by DHS cybersecurity experts, see JA 56 & n.3, JA 62-64. DHS also considered Section 1634 of the NDAA, which had been passed by both Chambers of Congress and submitted to the President for his signature. JA 56, 60-61; see https://go.usa.gov/xUXhc (congressional website identifying legislative and presidential actions concerning the NDAA).

Based on this review, DHS concluded that "[t]he record presents a compelling picture" of the risk posed by Kaspersky software on federal information systems. JA 79. Because Kaspersky's submission did not sufficiently mitigate the risks DHS

identified, DHS recommended that the Acting Secretary maintain the directive "without modification." JA 80. The Acting Secretary agreed, issuing a final decision on December 6, 2017 maintaining the directive without modification. JA 126-29.

III. LEGISLATIVE BACKGROUND

Congress was also concerned about the risks posed to federal information systems by Kaspersky products and services, in light of Russia's cyberattacks in the United States. Months before DHS issued the directive, Members of Congress expressed concern about Russia's use of cybertechnology "as a tool of warfare." *Disinformation: A Primer in Russian Active Measures and Influence Campaigns Panel II: Hearing Before the S. Comm. on Intelligence*, 115th Cong., pt. 2, 60 (2017) (*Disinformation*), https://go.usa.gov/xU5qv (statement of Sen. Harris); see *id.* at 42 (statement of Sen. Feinstein) (noting "major cyber attack on a presidential election in this country" by the Russian government, "including two intelligence services"). And some explicitly worried about the potential use by the Russian government of Kaspersky software. See *id.* at 40 (statement of Sen. Rubio) (discussing "open source reports" describing Kaspersky's "long history connecting them with" the FSB).

Members expressed concern about whether Kaspersky software was installed on federal information systems. *Open Hearing on Worldwide Threats: Hearing Before the S. Comm. on Intelligence*, 115th Cong. 65 (2017) (*Worldwide Threats*), https://go.usa.gov/xU5ch (statement of Sen. Manchin). And the Senate

Committee on Intelligence heard the heads of six U.S. intelligence agencies testify that they would not be comfortable with Kaspersky software on their computers. *Id.* at 48. In July, the Chairman of the House Committee on Science, Space, and Technology (House Science Committee) wrote to twenty-two federal agencies to express the Committee's concern "that Kaspersky Lab is susceptible to manipulation by the Russian government" and requesting information about the agencies' use of Kaspersky products or services on their information systems. Letter from Rep. Lamar Smith 1 (July 27, 2017), https://go.usa.gov/xU5xR (*Smith Letter*).

In October 2017, the House Science Committee held a hearing "to examine the concerns raised regarding the risks associated with utilizing Kaspersky Lab products on federal government information technology systems." *Bolstering the Government's Cybersecurity: Assessing the Risk of Kaspersky Lab Products to the Federal Government: Hearing Before the H. Subcomm. on Oversight, H. Comm. on Science, Space, and Technology*, 115th Cong. 3 (2017), https://go.usa.gov/xU5ad (*Bolstering I*). The committee chairman noted that "Kaspersky Lab is based in Moscow, Russia, and was founded in 1997 by Eugene Kaspersky." *Id.* at 8. The chairman further observed that Eugene Kaspersky was "educated at a KGB-sponsored university," he "wrote code for the Soviet military," and he reportedly "maintained close ties to Russian spies." *Id.* Among other things, the committee heard testimony from the Chief Information Officer at the U.S. General Services Administration, who testified

about the potential vulnerability posed by all antivirus software to federal information systems. *Id.* at 28 (testimony of David Shive). The committee also received expert witness testimony about the "legally mandated telecommunications monitoring for law enforcement and national security purposes" in Russia, which makes the risk posed by Kaspersky products "very real." *Id.* at 49 (statement of Sean Kanuck, Director for Future Conflict and Cyber Security, IISS-Americas) (Kanuck Statement); see *id.* (because of Russian law, "willful complicity may not be a required element of any foreign intelligence threat related to Kaspersky Lab").

The following month, a subcommittee of the House Science Committee held a hearing "to examine and assess the implementation of the Department of Homeland Security (DHS) Binding Operational Directive (BOD) 17-01 by federal government departments and agencies." *Bolstering the Government's Cybersecurity: A Survey of Compliance with the DHS Directive: Hearing Before the H. Subcomm. on Oversight, H. Comm. on Science, Space, and Technology*, 115th Cong. 3 (2017), https://go.usa.gov/xU5CA (*Bolstering II*). The committee heard testimony from, among others, DHS Assistant Secretary Manfra, who explained that the directive was based on the Department's concern about

> (1) the ties between certain Kaspersky officials and Russian intelligence and other government agencies, (2) requirements under Russian law that allow Russian intelligence agencies to request or compel assistance from Kaspersky and to intercept communications transiting Russian networks, and (3) the broad access to files and elevated privileges provided by anti-virus products

> and services, including Kaspersky products, that can be exploited by malicious cyber actors to compromise information systems.

Id. at 22 (statement for the record).

Against this backdrop, during consideration of the NDAA for the 2018 fiscal year, the Senate Armed Services Committee initially proposed a limited provision addressing cybersecurity that "would prohibit any component of the Department of Defense from using" any Kaspersky software. S. Rep. No. 115-125, at 302 (2017), https://go.usa.gov/xU5uH; see *id.* at 296. The committee stated that it "believes that the United States must do more to deter Russian aggression" including "in cyberspace," and that the provision would "[p]rohibit[] DOD from using software platforms developed by Kaspersky Lab due to reports that the Moscow-based company might be vulnerable to Russian government influence." Senate Armed Services Comm., *NDAA FY18 Executive Summary*, 9, 10 (2017), https://go.usa.gov/xU5JC (*Executive Summary*).

Eventually, after months of investigating and gathering information about the risk Kaspersky products pose to federal information systems, Congress enacted Section 1634 as part of the NDAA. Section 1634(a) prohibits any federal entity from using "any hardware, software, or services developed or provided, in whole or in part, by" Kaspersky or any entity controlled by Kaspersky. Section 1634(b) makes the prohibition effective October 1, 2018. And Section 1634(c) requires the

Secretary of Defense, in consultation with other agencies, to "conduct a review of the procedures for removing suspect products or services from the information technology networks of the Federal Government" and to report the result of that review to specified congressional committees, including an assessment of any gaps in agency authority to remove such products or services.

IV. PRIOR PROCEEDINGS

Days after Congress enacted Section 1634, Kaspersky brought the first suit. The suit challenged the directive under the APA, contending that DHS employed constitutionally deficient procedures in issuing the directive and that issuance of the directive was arbitrary and capricious because it was unsupported by substantial evidence. JA 21-22. After the government argued that Kaspersky lacks standing to challenge the directive in light of the enactment of Section 1634, which independently prohibits the use of Kaspersky products by federal entities, plaintiffs filed a separate suit, challenging Section 1634 as an unconstitutional bill of attainder. JA 149-50. After consolidating the cases for the purpose of briefing dispositive motions, the district court dismissed both suits. JA 169-223.

The district court dismissed Kaspersky's challenge to Section 1634 on the merits, concluding that the complaint failed to state a claim. JA 192-214, 223. The Bill of Attainder Clause prohibits legislation, the district court observed, only if it both applies with specificity and imposes punishment. JA 192 (discussing *Foretich v.*

United States, 351 F.3d 1198, 1217 (D.C. Cir. 2003)). Although Section 1634 applies with specificity to plaintiffs (JA 193), the district court determined that the provision does not impose any punishment because its requirements do not represent the kind of deprivations and disabilities historically associated with bills of attainder (JA 194-201); because it rationally furthers nonpunitive legislative purposes (JA 201-08); and because the legislative record evinced no congressional intent to punish (JA 208-14). See *Foretich*, 351 F.3d at 1218. The district court separately concluded that, in light of the validity of Section 1634, plaintiffs lack standing to challenge the BOD, and it dismissed the BOD suit for lack of jurisdiction. JA 214-23.

Kaspersky appealed the dismissal of both suits. Concurrent with the filing of its opening brief, Kaspersky filed an emergency motion seeking an injunction pending appeal, which this Court denied.

SUMMARY OF ARGUMENT

1. a. The district court correctly held that Section 1634 is not an unconstitutional bill of attainder. To qualify as a bill of attainder, a statute must impose legislative punishment on an identifiable individual. While Section 1634 specifies a prohibition on the use of Kaspersky products and services, the statute is not a bill of attainder because it imposes no punishment under any of the three applicable tests. First, the statute does not impose a deprivation that comes within

the historic examples of bills of attainder. In particular, Section 1634 does not prevent Kaspersky from engaging in a profession, nor is it an employment bar. Second, and most importantly, Section 1634 is not functionally a bill of attainder. The provision has the legitimate, nonpunitive purpose of mitigating the risk of successful cyberattacks on federal information systems. And Congress's response to that risk is rationally related and proportional to the statute's purpose. Third, the legislative background unambiguously shows that Congress's motivation in enacting the statute was preventive, not punitive.

b. Kaspersky's contrary arguments lack merit. First, Kaspersky claims that Section 1634 necessarily marks it with a brand of disloyalty. But Congress's determination that the government's use of a company's product poses a national security risk and its prohibition on the use of that product does not necessarily reflect any improper legislative opprobrium of the company. Section 1634 is based on a determination that features of the company's product make it susceptible to misuse, and there is no reason to extend the rationale underlying the employment-bar cases to the quite different context of this case. Second, Kaspersky offers no support for its suggestion that Congress did not, in fact, enact Section 1634 to address a national-security vulnerability. To suggest that legislation cannot address a national-security concern until the national-security harm is proven is implausible on its face. And the only less-burdensome alternative Kaspersky identifies would not

fully remedy the harm Congress identified. Third, the only materials on which Kaspersky relies related to Congress's motivation cannot objectively be described as showing a punitive intent.

c. Finally, Kaspersky's procedural arguments are flawed because the court was not required to accept as true legal conclusions in a complaint that are couched as factual allegations, and because the court properly took judicial notice of public documents.

2. a. The district court also correctly held that it lacked jurisdiction to consider Kaspersky's challenge to the directive, because any favorable decision would not redress Kaspersky's alleged injuries. The court properly exercised its discretion in considering first the logically antecedent question of the constitutionality of Section 1634. Having upheld the validity of that statute, the district court correctly determined that Kaspersky could obtain no redress from a favorable ruling concerning the directive, because the prohibition in Section 1634 is broader than that in the directive. Whether viewed through the lens of standing or mootness, Kaspersky's challenge to the directive is not justiciable.

b. In any event, even if there were jurisdiction, Kaspersky fails to state a procedural due-process claim on which relief may be granted. Procedural due process requires notice of the proposed official action, including the factual basis for the action, and an opportunity for the affected party to respond. In this case, the

Acting Secretary's decision memorandum, the directive, and the First Manfra Memorandum served as notice of DHS's plan to require federal agencies to begin to remove Kaspersky-branded products ninety days after issuance of the directive, and it provided he factual basis for that intended action. DHS set up an administrative process through which Kaspersky could respond and rebut the agency's decision, and Kaspersky took full advantage of that administrative remedy. DHS considered and addressed Kaspersky's submission before issuing a final decision. That is all the process this Court's precedent requires.

c. Kaspersky argues that the district court's jurisdictional decision was erroneous because Kaspersky suffered injury when DHS issued the directive. But even if Kaspersky could have identified a sufficient injury, traceable to the directive and redressable by the court, to demonstrate standing prior to the enactment of Section 1634, it could not do so at the time the suit was initiated. In any event, there is no cognizable injury now as a consequence of the directive, and a plaintiff must maintain a sufficient personal interest throughout the course of the litigation, for the court to have jurisdiction. Kaspersky speculates that invalidation of the directive would have partially remedied its alleged injuries. But that assertion is based on mere speculation, and Kaspersky provides no concrete reason to support the contention.

STANDARD OF REVIEW

This Court "review[s] the district court's dismissal of a complaint for lack of standing or for failure to state a claim *de novo*." *Washington Alliance of Tech. Workers v. United States Dep't of Homeland Security*, 892 F.3d 332, 339 (D.C. Cir. 2018).

ARGUMENT

I. SECTION 1634 IS NOT A BILL OF ATTAINDER

Article I, Section 9 of the United States Constitution prohibits Congress from enacting bills of attainder, laws "that legislatively determine[] guilt and inflict[] punishment upon an identifiable individual without provision of the protections of a judicial trial." *Nixon v. Administrator of Gen. Servs.*, 433 U.S. 425, 468 (1977); see U.S. Const. art. I, § 9, cl. 3.[3] But it is not enough that a statute affects a specific individual: "[S]pecificity alone does not render a statute an unconstitutional bill of attainder." *Foretich v. United States*, 351 F.3d 1198, 1217 (D.C. Cir. 2003); see

[3] Kaspersky's constitutional claim would face another hurdle because the Bill of Attainder Clause concerns "legislative interferences[] in cases affecting personal rights." *United States v. Brown*, 381 U.S. 437, 444 n.18 (1965) (quoting *The Federalist*, No. 44, at 351 (James Madison) (Hamilton ed. 1980)). Neither the Supreme Court nor this Court has applied the Bill of Attainder Clause to corporations. See *BellSouth Corp. v. Federal Commc'n Comm'n*, 162 F.3d 678, 684 (D.C. Cir. 1998) (*BellSouth II*) (so assuming without deciding the issue). Because it is clear that Section 1634 does not impose punishment on Kaspersky, the Court need not resolve the question in this case. However, because "it is obvious that there are differences between a corporation and an individual under the law," any analogy to prior bill-of-attainder cases "that have involved individuals * * * must necessarily take into account this difference." *Id.*

Nixon, 433 U.S. at 471-72 ("[T]he Act's specificity—the fact that it refers to appellant by name—does not automatically offend the Bill of Attainder Clause."). That is because the Bill of Attainder Clause "was not intended to serve as a variant of the equal protection doctrine, invalidating every Act of Congress or the States that legislatively burdens some persons or groups but not all other plausible individuals." *Nixon*, 433 U.S. at 471. A law that is a bill of attainder must not only apply with specificity, it must also impose punishment. *Foretich*, 351 F.3d at 1217.

"Forbidden legislative punishment is not involved merely because the Act imposes burdensome consequences." *Nixon*, 433 U.S. at 472. Rather, courts must inquire whether a statute "inflict[s] punishment within the constitutional proscription." *Id.* at 472-73 (quotation marks omitted). The three-part inquiry governing that question applies the historical, functional, and motivational tests of punitiveness, asking respectively "(1) whether the challenged statute falls within the historical meaning of legislative punishment; (2) whether the statute, viewed in terms of the type and severity of burdens imposed, reasonably can be said to further nonpunitive legislative purposes; and (3) whether the legislative record evinces a congressional intent to punish." *Foretich*, 351 F.3d at 1218 (quotation marks omitted). "[T]hose [three] factors are the evidence that is weighed together in resolving a bill of attainder claim." *Id.* (quoting *Consolidated Edison Co. v. Pataki*, 292 F.3d 338, 350 (2d Cir. 2002)) (quotation marks omitted). The "functional test

* * * invariably appears to be the most important of the three." *Id.* (quotation marks omitted). And because "[j]udicial inquiries into Congressional motives are at best a hazardous matter," courts should hesitate to find a constitutional violation under the motivational test. *Flemming v. Nestor*, 363 U.S. 603, 617 (1960); see *id.* ("only the clearest proof could suffice to establish the unconstitutionality of a statute" based on the motivational test).

There is no dispute in this case that Section 1634 applies to plaintiffs with specificity. But the district court correctly determined that the statute does not impose punishment, and therefore is not an unconstitutional bill of attainder.

A. Section 1634 Does Not Impose Punishment on Kaspersky

1. Under the historical test, courts consult "a ready checklist of deprivations and disabilities so disproportionately severe and so inappropriate to nonpunitive ends that they unquestionably have been held to fall within the proscription of" the Bill of Attainder Clause. *Nixon*, 433 U.S. at 473. "This checklist includes sentences of death, bills of pains and penalties, and legislative bars to participation in specified employments or professions."[4] *Foretich*, 351 F.3d at 1219. It is plain that Section

[4] "Generally addressed to persons considered disloyal to the Crown or State, 'pains and penalties' historically consisted of a wide array of punishments: commonly included were imprisonment, banishment, and the punitive confiscation of property by the sovereign." *Nixon*, 433 U.S. at 474 (footnotes omitted).

1634 does not sentence anyone to death and imposes no historical pains and penalties. And there is little question that the statute does not, in the relevant sense, bar Kaspersky from participation in any employment or profession.

First, it is obvious that Section 1634 does not prohibit Kaspersky from engaging in a profession. Kaspersky "is not prevented from operating as a cybersecurity business. * * * The company may still operate and derive revenue throughout the world, including in the United States, by selling its products to individuals, private companies, and other governments." JA 197.

Second, this Court has rejected the claim that a legislative restriction on a company's ability to enter a specific line of business is tantamount to the permanent exclusion of an individual from a particular occupation. See *BellSouth Corp. v. Federal Commc'ns Comm'n*, 144 F.3d 58, 64-65 (D.C. Cir. 1998) (*BellSouth I*) (describing as "very loose indeed" the analogy to "traditional employment debarments"); see *BellSouth II*, 162 F.3d at 684 (noting the need to "take into account th[e] difference" between corporations and individuals in considering bill-of-attainder claims). It necessarily follows that a restriction prohibiting the U.S. government from entering into discretionary contracts with a particular corporation—while leaving the corporation fee to engage in its chosen line of business—is nothing like the individual employment-bar cases. See *BellSouth I*, 144

F.3d at 65 (statute that leaves corporation "free to pursue" its chosen business not a bill of attainder); see generally JA 195-201.

Third, "[w]hen the Court extended 'punishment' to include employment bars, it did so because it was concerned that the government had imposed restrictions that violated the fundamental guarantees of political and religious freedom." *BellSouth II*, 162 F.3d at 686; see, *e.g.*, *Brown*, 381 U.S. at 438-39 (statute making it a crime for a member of the Communist Party to serve as an officer or an employee of a labor union is a bill of attainder); *United States v. Lovett*, 328 U.S. 303, 313-14 (1946) (statute barring individuals from government employment upon determination by a congressional subcommittee that they are guilty of subversive activity is a bill of attainder). Kaspersky does not claim that Section 1634 burdens anyone's political or religious freedom, no comparable constitutional guarantees are implicated by the statute's prohibition, and, in any event, Kaspersky identifies no constitutional right that it alleges is infringed by Section 1634.

And fourth, in the employment-bar cases, "the individuals involved were in fact being punished for past actions." *American Commc'ns Ass'n, C.I.O. v. Douds*, 339 U.S. 382, 413 (1950). Where Congress legislates "to prevent future action rather than to punish past action," and there are "substantial ground[s] for the congressional judgment," the distinction is "decisive"; the statute is not a bill of

attainder. *Id.* at 413-14; see also *Flemming*, 363 U.S. at 614.[5] As we next explain, Congress enacted Section 1634 to mitigate a significant risk to federal information systems rather than to punish Kaspersky for any past action, and substantial grounds supported Congress's decision to enact that provision.

2. Under the functional test, courts consider "whether the law under challenge, viewed in terms of the type and severity of burdens imposed, reasonably can be said to further nonpunitive legislative purposes." *Foretich*, 351 F.3d at 1220 (quotation marks omitted). The inquiry examines "both the purported ends of [the] contested legislation and the means employed to achieve those ends." *Id.* at 1221. If there is a "legitimate nonpunitive purpose and a rational connection between the burden imposed and nonpunitive purposes of the legislation," then the statute is not a bill of attainder under the functional test. *Id.*

It is clear on the face of the statute that Section 1634 has a legitimate nonpunitive purpose: mitigating the risk of successful cyberattacks on federal information systems. See *Trump v. International Refugee Assistance Project*, 137 S. Ct. 2080, 2088 (2017) (per curiam) ("The interest in preserving national security is an

[5] *Nixon* recognized that, where there are *not* substantial grounds for preventive legislation, and such legislation is instead based on disapproval of the political or other beliefs of the targeted individual, the future-focus of the legislation will not preclude a determination that it is a bill of attainder. 433 U.S. at 476 n.40.

urgent objective of the highest order.") (quotation marks omitted). Section 1634 is part of Subtitle C of the NDAA, which is devoted to "Cyberspace-Related Matters." Section 1633 directs the Executive to establish a national policy concerning, among other things, cybersecurity. NDAA § 1633(a)(1). The policy must identify the available resources "to deter or respond to cyber attacks or other malicious cyber activities by a foreign power or actor that targets United States interests," responses to such attacks, and options to "prioritize the defensibility and resiliency against cyber attacks" against critical infrastructure. NDAA § 1633(b)(1)-(3). In that context, and toward similar ends, Congress prohibited government agencies from using hardware, software, and services developed or provided, in whole or in part, by Kaspersky. NDAA § 1634(a).

Congress's purpose in enacting Section 1634 was not limited to addressing Kaspersky products. After prohibiting the use of covered Kaspersky products and services, Congress directed the Secretary of Defense, in consultation with other agency heads, to conduct a broader "review of the procedures for removing suspect products or services from the information technology networks of the Federal Government." NDAA § 1634(c)(1). Section 1634 further requires the Defense Secretary to submit a report to specified congressional committees identifying the authorities federal agencies have for preventing the use of any "suspect products or services" and to identify "any gaps" in that authority. NDAA § 1634(c)(2)(B)(i) &

(ii). Thus, in Section 1634, Congress identified a specific threat and directed federal agencies to take action mitigating the risk posed by that threat, but Congress also recognized that there might be other, similar threats and it directed the Department of Defense to address them.

The statute itself therefore manifests Congress's legitimate intent to mitigate the risk to federal information systems posed by the presence of Kaspersky products and services on those systems. Congress provided federal agencies with an unambiguous statutory prohibition against the use of Kaspersky products and services; it directed the submission of a report outlining the existing authorities on which federal agencies may rely to prohibit the use of other suspect products or services; and it called for the identification of any gaps in those authorities—presumably to permit Congress to enact any needed remedial legislation.

Further, it is equally clear that the means Congress chose to address the legitimate legislative purposes are rationally related and proportional. Congress was concerned that the government's use of Kaspersky software and services creates a national-security risk. It therefore prohibited the use of such software and services on federal information systems. But it imposed no other limitation on Kaspersky's ability to conduct business in the United States. The means Congress chose are therefore directly responsive to the problem that concerned it. For the same reason, the burden Section 1634 imposes on Kaspersky is not a "grave imbalance" that

might suggest punitive intent. *Foretich*, 351 F.3d at 1222. As the district court observed, Kaspersky only "is prevented from seeking discretionary contracts from the United States federal government." JA 197; see *Navegar, Inc. v. United States*, 192 F.3d 1050, 1067 (D.C. Cir. 1999) ("[M]erely because a regulation is burdensome does not mean that it constitutes punishment."). Because Congress adopted means proportional to the harm it sought to address, Section 1634 is not a bill of attainder under the functional test. See generally JA 201-208.

3. Finally, Section 1634 does not qualify as a bill of attainder under the motivational test. Nothing in the "legislative history, the context or timing of the legislation, or specific aspects of the text or structure," *Foretich*, 351 F.3d at 1225, suggests any intent to punish Kaspersky.

The legislative background relating to the enactment of Section 1634, discussed above, see *supra* pp. 9-13, unambiguously shows that Congress's purpose in enacting the provision was preventive, not punitive. Nothing in the legislative record even hints at any intent to punish Kaspersky for some "blameworthy offense[]." *Foretich*, 351 F.3d at 1225 (quotation marks omitted). Congress enacted Section 1634 after months of inquiry, including hearings at which high-ranking members of the intelligence community testified, as did cybersecurity experts, concerning the risks posed to federal information systems by Kaspersky software and services.

The context and timing likewise offer no suggestion that Congress intended to punish Kaspersky. When Congress adopted the provision, various congressional committees, like the Senate Armed Services Committee, were concerned about "Russian aggression" including "in cyberspace," and they were contemplating measures to minimize risks of Russian government attacks on federal information systems. *Executive Summary* 9, https://go.usa.gov/xU5JC. Section 1634 was enacted in that context, and in response to Congress's recognition that cyberintrusions attributed to the Russian government were recent and ongoing. See generally, *e.g.*, *Disinformation*, https://go.usa.gov/xU5qv. Finally, nothing in the text of Section 1634 or the structure of the NDAA even hints at a punitive purpose. As discussed above, see *supra* pp. 23-25, the text of the provision and its placement in a subtitle addressing cybersecurity disclose Congress's intent to address what it perceived to be a pressing national-security risk. Section 1634 thus does not qualify as a bill of attainder under the motivational test. See generally, JA 208-14.

In sum, Section 1634 furthers a legitimate, nonpunitive purpose: to mitigate risks to federal information systems from products and services that might be used by the Russian government to harm national-security interests. As the district court correctly determined, "[w]eighing all three tests for punishment together, * * * Sections 1634(a) and (b) of the NDAA clearly do not inflict punishment" on Kaspersky. JA 214.

B. Kaspersky's Contrary Arguments Lack Merit

1. Kaspersky argues that Section 1634 qualifies as an example of the historic legislative deprivations that qualify as bills of attainder because it "singles out and targets Kaspersky Lab," "brands Kaspersky Lab with infamy and disloyalty," and is "consistent with" an extension of the "historical forms of punishment." Br. 15, 17, 19 (formatting altered). Those arguments are incorrect.

a. Kaspersky acknowledges that the specificity of a statute is not sufficient to make it an unconstitutional bill of attainder. Br. 15. It argues, however, that Congress's identification of Kaspersky "raises suspicion" about Congress's punitive intent. *Id.* (quoting *Foretich*, 351 F.3d at 1224); see *id.* at 15-16. But the statute's specificity does not raise any suspicion if, "viewed in context, the focus of the enactment can be fairly and rationally understood." *Nixon*, 433 U.S. at 472; see *id.* at 471-72 (noting that the statute "refers to appellant by name"). In that event, the subject of the legislation will "constitute[] a legitimate class of one," which, in appropriate circumstances, may justify "Congress' decision to proceed with dispatch." *Id.* at 472. For the reasons provided above, the focus of Section 1634 can easily be fairly and rationally understood. Because the statute has a legitimate purpose, and Congress rationally identified government use of Kaspersky products as a threat to national security, the specificity of Section 1634 raises no suspicion that Congress intended to single out Kaspersky for punishment. See *BellSouth I*, 144

F.3d at 67 (stating that "the differential treatment of the [Bell Operating Companies] and [non-Bell Operating Companies] is neither suggestive of punitive purpose nor particularly suspicious" in light of the characteristics of the former and the problem Congress sought to address); *id.* ("[T]he distinction drawn by Congress seems quite understandable without resort to inferences of punitive purpose.").

b. Kaspersky next argues that Section 1634 "stamp[s] it with Congress's legislative conclusion that the company is disloyal to the United States." Br. 17. Kaspersky suggests that Congress "prohibited the use of Kaspersky Lab products and services on government systems because it considered, without a judicial determination of guilt or blameworthiness, that Kaspersky Lab products and services create an 'alarming national security vulnerability.'" Br. 17-18 (quoting JA 156 (Jeanne Shaheen, Opinion, *The Russian Company That Is a Danger to Our Security*, N.Y. Times, Sept. 4, 2017) (Shaheen Opinion)). "There is," Kaspersky opines, "no other explanation for the prohibition." *Id.* That argument is incorrect.

First, Kaspersky's equation of a legislative determination of a national-security vulnerability with a legislative determination of guilt or blameworthiness is obviously ill conceived. Congress's determination that the government's use of a company's product on federal systems poses a national-security risk and its prohibition of government agencies using that product does not necessarily (and not even inferentially) suggest legislative opprobrium of the company. Instead, Congress can

be expected to take such a step based simply on a determination that features of the company's product make it susceptible to misuse. That is the obvious "other explanation" that Kaspersky finds elusive. Indeed, as Kaspersky "repeatedly emphasize[d]" in the district court, Section 1634 "appears to have nothing to do with any finding that Kaspersky Lab has done anything wrong or disloyal." See JA 200. And the correctness of Congress's determination is beside the point: "Congress may read the evidence before it in a different way than might this court or any other, so long as it remains clear that Congress was pursuing a legitimate nonpunitive purpose." *BellSouth II*, 162 F.3d at 689.

Second, Kaspersky's suggestion that Congress could not make such a determination without first obtaining a "judicial determination," Br. 17-18, seriously misunderstands the respective roles of the courts and the political branches. It is undoubtedly the courts' role to determine in national security matters whether Congress and the Executive have acted within constitutional bounds. But it is equally clear that the Constitution commits to the political branches the authority to evaluate and act on national security risks, and requires the courts to give substantial deference to the political branches' national security determinations. See, *e.g.*, *Zadvydas v. Davis*, 533 U.S. 678, 696 (2001) (noting the "heightened deference to the judgments of the political branches with respect to matters of national security"); *Larson v. Department of State*, 545 F.3d 857, 865 (D.C. Cir. 2009) (stating that this

Court has "found it unwise to undertake searching judicial review" of Executive Branch predictions concerning "harm to the national security").[6]

c. Kaspersky contends that the district court erred in considering only specific historic examples of legislative punishment and, in doing so, "applied the historical test too narrowly." Br. 20. Kaspersky correctly observes that this Court has not narrowly limited the historic test to the checklist of statutory deprivations and disabilities previously deemed to be bills of attainder. When considering whether it would be appropriate to "exten[d]" the historical category, the Court has considered whether the statutory burden in question "is not dissimilar to the types of burdens traditionally recognized as punitive." *Foretich*, 351 F.3d at 1220. But that approach does not avail Kaspersky because there is no basis to extend the historical test to reach Section 1634.

Kaspersky seeks the extension of "the types of burdens traditionally recognized as punitive" (*Foretich*, 351 F.3d at 1220), in the employment-bar cases (Br. 22-23). But this Court has explained that those cases were themselves an extension of

[6] Kaspersky asserts that Congress enacted Section 1634 only on the basis of "unsubstantiated rumors." Br. 19. But that contention is plainly belied by the legislative record, which demonstrates that congressional committees carefully investigated the threat posed by Kaspersky software and services, receiving testimony and submissions from the most senior officials of the government's national security agencies as well as from experts in the private sector. See *supra* pp. 9-13.

historical notions of punishment. *See BellSouth* II, 162 F.3d at 686. And the rationale for that extension does not apply here: "When the Court extended 'punishment' to include employment bars, it did so because it was concerned that the government had imposed restrictions that violated the fundamental guarantees of political and religious freedom." *Id.*; *Navegar*, 192 F.3d at 1067 (same). Kaspersky makes no claim that Section 1634 violates any guarantee of political or religious freedom. Moreover, in the employment-bar cases, "the individuals involved were in fact being punished for past actions." *American Commc'ns Ass'n*, 339 U.S. at 413. Kaspersky nowhere disputes that Congress enacted Section 1634 "to prevent future action rather than to punish past action." *Id.* at 414. Because that distinction is "decisive," *id.* at 413, Kaspersky has failed to demonstrate that it would be appropriate to extend the rationale underlying the employment-bar cases even further to encompass legislation enacted to mitigate a national security risk.[7]

2. Kaspersky contends that Congress did not, in fact, enact Section 1634 to mitigate a national security risk it identified and that the burdens imposed on

[7] Kaspersky seeks to distinguish the cases in which this Court "declin[ed] to expand the category of historical punishments" as resting on the possibility that the legislative restriction could be overcome. Br. 24 (formatting altered); see Br. 24-26. But even if that feature distinguishes those cases from this one, Kaspersky has still failed to demonstrate that it would be appropriate to extend the rationale of the employment-bar cases to encompass Section 1634.

Kaspersky do not, in any event, reasonably further that legislative purpose. Br. 26-37; see *Foretich*, 351 F.3d at 1220 ("[The functional test asks] whether the law under challenge, viewed in terms of the type and severity of burdens imposed, reasonably can be said to further nonpunitive legislative purposes."). Kaspersky's arguments are meritless.

a. Kaspersky does not dispute that protecting against national security risks is "an urgent objective of the highest order." *International Refugee Assistance Project*, 137 S. Ct. at 2088. Instead, Kaspersky appears to contend that Congress did not enact Section 1634 for that purpose. Br. 27-29. But Kaspersky's only support for that contention is its bare assertion that Congress enacted the provision "to purge Kaspersky Lab from [federal] information systems based on unproven and unfounded allegations that it poses a cyberthreat." Br. 29; see Br. 35 ("[T]here is no conclusive evidence that Kaspersky Lab has caused any breach at all."). But that argument merely quibbles with Congress's evaluation of the national security risk; it does not demonstrate that Congress had any different purpose.

The idea that the federal government must wait until it can "prove" a national security harm before it can act to address what it perceives as a significant risk is remarkable, and demonstrably incorrect. Notably, Kaspersky cites no authority for the idea that Congress is precluded from taking steps to prevent a national-security threat before the nation suffers the consequences of that threat. The political

branches' national security actions are based on expert "agency judgments on potential risks to national security." *Olivares v. Transportation Sec. Admin.*, 819 F.3d 454, 462 (D.C. Cir. 2016). "[C]ourts do not second-guess" those judgments but instead "defer to the informed judgment of agency officials whose obligation it is to assess risks to national security." *Id.*; see also, *e.g.*, *Larson*, 565 F.3d at 865 ("[W]e have consistently deferred to executive affidavits predicting harm to the national security, and have found it unwise to undertake searching judicial review.") (alteration in original).

Kaspersky's disagreement with the government's assessment of the national-security risk has no bearing on whether Section 1634 has a nonpunitive legislative purpose. Congress undertook months of investigations; held multiple hearings; and heard testimony and received submissions from multiple senior national security officials, including from the heads of six intelligence agencies. See *supra* pp. 9-13. Congress had ample foundation for Section 1634 in the expert, predictive judgments of executive branch officials entrusted with protecting the national security. *Cf.*, *e.g.*, *BellSouth II*, 162 F.3d at 689 ("Congress may read the evidence before it in a different way than might this court or any other, so long as it remains clear that Congress was pursuing a legitimate nonpunitive purpose.").

Kaspersky's reliance on the employment-bar cases (Br. 28-29) to suggest that courts should look behind the political branches' national-security determinations

also is meritless. First, as noted (see *supra* pp. 22), Kaspersky identifies no constitutional right that it alleges to be infringed by Section 1634, which is the rationale underlying the employment-bar cases. See *BellSouth II*, 162 F.3d at 686. Second, there was no suggestion in those cases, as in this one, that Congress had established a legislative record demonstrating its good-faith determination that the regulated conduct would pose a significant national security risk. See *supra* pp. 9-13, and *infra* p. 36. Finally, Kaspersky identifies nothing improper about that determination, besides innuendo.

b. Kaspersky's complaint alleged, and its brief argues, that Section 1634 is causing it reputational harm and a loss of sales. JA 149; Br. 29-32, 34-35. However, "[i]t is not the severity of a statutory burden in absolute terms that demonstrates punitiveness so much as the magnitude of the burden relative to the purported nonpunitive purposes of the statute." *Foretich*, 351 F.3d at 1222.; see *Linnas v. Immigration & Naturalization Serv.*, 790 F.2d 1024, 1030 (2d Cir. 1986) ("Severity * * * does not in itself make a burden a punishment."). The question, instead, is whether there is "a rational connection between the burden imposed and nonpunitive purposes of the legislation."[8] *Foretich*, 351 F.3d at 1221; see *Patchak v.*

[8] Kaspersky criticizes the district court for only considering, as Kaspersky puts it, whether there was "some 'rational' reason for Section 1634(a)." Br. 27 n.11. But that misdescribes the district court's opinion. After having determined that Section

Jewell, 828 F.3d 995, 1006 (D.C. Cir. 2016) ("[T]he means employed by the statute must be rationally designed to meet its legitimate nonpunitive goals.").

As the district court aptly summarized (JA 202-03), when Congress enacted Section 1634 it had

- conducted hearings concerning Russian cyberattacks and influence campaigns against the United States; see generally *Disinformation*, https://go.usa.gov/xU5qv;
- sought information about agencies' use of Kaspersky products or services on their information systems; see, *e.g.*, *Smith Letter*, https://go.usa.gov/xU5xR;
- held hearings concerning the national security risks Kaspersky software and services pose to federal information systems; see generally *Bolstering I*, https://go.usa.gov/xU5ad; *Bolstering II*, at 22, https://go.usa.gov/xU5CA;
- heard testimony concerning the requirements of Russian law that could enable Russian intelligence agencies to intercept information sent to Kaspersky servers in Russia or otherwise expose federal information system to cyberattack by the Russian government; *Bolstering I*, at 29, https://go.usa.gov/xU5ad; *Bolstering II*, at 22, https://go.usa.gov/xU5CA; and
- took testimony and otherwise noted the connection between Kaspersky officials and Russian intelligence and other government agencies; *Bolstering I*, at 8, https://go.usa.gov/xU5ad; *Bolstering II*, at 22, https://go.usa.gov/xU5CA.

1634 has a nonpunitive purpose, the district court correctly determined that the burdens imposed on Kaspersky are rationally related to that purpose. See, *e.g.*, JA 203 ("It is sufficient for this Court to say that it was rational for Congress to conclude on the basis of this information that barring the federal government's use of Kaspersky Lab products would help prevent further Russian cyber-attacks.").

In light of the totality of these considerations, Congress was entitled to exercise its judgment to mitigate what it perceived to be the national security risk to federal information systems uniquely posed by government use of Kaspersky software and services. And it is plain that a statutory requirement prohibiting the use on federal information systems of Kaspersky software and services is directly targeted at, and so rationally related to, the risk Congress sought to address.

Finally, Kaspersky argues that there is a "grave imbalance" between the burden it suffers and the nonpunitive purpose of Section 1634, thus suggesting punitiveness. Br. 34 (quoting *Foretich*, 351 F.3d at 1222). The imbalance, Kaspersky contends, stems from Section 1634's overbreadth (Br. 32-36) and its failure to impose less-burdensome alternatives (Br. 36-37). The only less-burdensome alternative Kaspersky identifies (Br. 36) is "debarment" under the Federal Acquisition Regulation, regulations that govern federal contracting. See 48 C.F.R. § 9.406 ("Debarment"). But debarment applies only to future contracts. See 48 C.F.R. § 9.405 ("Effect of listing"). It would not have required federal entities to remove Kaspersky software or services from federal information systems, nor would it have prevented resellers or other contractors from selling Kaspersky products or services to the federal government. It was therefore reasonable for Congress to conclude that debarment would not adequately mitigate the national security risk caused by the use of Kaspersky software and services by the federal government.

Kaspersky argues that Section 1634 is overbroad because Congress did not permit the use of some products, like its "threat intelligence and research reports," that Kaspersky asserts do not pose a risk to federal information systems. Kaspersky also argues that the prohibition improperly applies "across the entire federal government." Br. 33, 34. But neither the Supreme Court nor this Court has held that the functional test requires Congress to adopt the least restrictive means to further its legitimate nonpunitive ends. Instead, the question is whether a "rational and fairminded Congress" could have enacted the statute to address the problem it identified. *Nixon*, 433 U.S. at 483; see *Foretich*, 351 F.3d at 1222-23 ("Congress must have sufficient latitude to choose among competing policy alternatives so that our bill of attainder analysis will not 'cripple the very process of legislating.'") (quoting *Nixon*, 433 U.S. at 470). A fair-minded Congress could rationally have concluded that government use of any hardware, software, or services developed or provided in whole or in part by Kaspersky increased the risk of a successful Russian cyberattack, and that a general prohibition applicable to all federal information systems is necessary to mitigate that risk. Moreover, because the alternative Kaspersky itself identifies (Br. 36-37) as less burdensome—debarment—would itself have imposed similar burdens by preventing Kaspersky from transacting any business with any government agency, the overbreadth argument does not demonstrate that Section 1634 is improperly punitive. See 48 C.F.R. § 9.405(a).

For these reasons, Kaspersky has failed to show that Section 1634 is a bill of attainder under "the most important," functional test. *Foretich*, 351 F.3d at 1218; see generally JA 201-08.

3. Relying entirely on a few statements by Jeanne Shaheen, the Senate sponsor of Section 1634, Kaspersky contends that Congress had a punitive motivation when enacting the provision. As an initial matter, "'[s]everal isolated statements' are not sufficient to evince punitive intent." *BellSouth II*, 162 F.3d at 690 (quoting *Selective Serv. Sys. v. Minnesota Pub. Interest Research Grp.*, 468 U.S. 841, 856 n.15 (1984)). And because the motivational test "by itself is not determinative in the absence of unmistakable evidence of punitive intent," *Foretich*, 351 F.3d at 1225 (quotation marks omitted), even if Senator Shaheen's statements could be read to suggest an intent to punish Kaspersky, that would not establish that Section 1634 is itself punitive, in light of the outcome of the historical and functional tests.

In any event, the statements Kaspersky identifies cannot objectively be described as showing any punitive intent. Kaspersky relies (Br. 38-39) on the following statements:

- "The Russian Company That Is a Danger to Our Society," Br. 38 (quoting JA 156 (title of Shaheen Opinion));
- "Kaspersky Lab's products create an 'alarming national security vulnerability,'" *id.* (quoting JA 156 (text from Shaheen Opinion));

- "Kaspersky Lab, with an active presence in millions of computer systems in the United States, is capable of playing a powerful role in [] an assault [on critical American infrastructure]"; *id.* (quoting JA 158 (text from Shaheen Opinion)) (alterations added by Kaspersky);

- "[T]he case against Kaspersky is overwhelming. * * * [T]he strong ties between Kaspersky Lab and the Kremlin are alarming and well-documented. * * * [M]y amendment * * * removes a real vulnerability to our national security," Br. 39 (quoting JA 162 (Press Release, *Shaheen's Legislation to Ban Kaspersky Software Government-Wide Passes Senate as Part of Annual Defense Bill* (Sept. 18, 2017), https://go.usa.gov/xUdZ5)).

These statements unambiguously express concern about the "threat to our national security" posed by Kaspersky products and a desire to take steps to mitigate that threat. JA 158 (text from Shaheen Opinion). They also reflect not even the slightest suggestion that Senator Shaheen sponsored Section 1634 to punish Kaspersky.[9] *Accord* JA 211.

The district court thus correctly concluded that the motivational test lends no support to Kaspersky's contention that Section 1634 is a bill of attainder. See generally JA 208-214.

---

[9] Kaspersky additionally relies on a recent statement by Senator Shaheen that "[s]anctioning Kaspersky Lab is a logical next step." Br. 39 n.16. (quoting Joe Uchill, *US mulls sanctions against Kaspersky Lab*, Axios (Apr. 23, 2018), https://goo.gl/UtMgTe). That statement, Kaspersky contends, demonstrates "a larger effort to punish Kaspersky Lab." *Id.* Even assuming that the statement suggests Senator Shaheen's intent to punish Kaspersky (something we do not concede), such "postenactment statements" even by a "key sponsor[]" of a bill "cannot possibly have informed the vote of the legislators who earlier enacted the law." *Pittson Coal Grp. v. Sebben*, 488 U.S. 105, 118-19 (1988).

C. Kaspersky's Procedural Arguments Also Lack Merit

Kaspersky argues (Br. 40-47) that the district court committed reversible procedural errors in granting the government's motion to dismiss Kaspersky's challenge to Section 1634. "[F]aced with a Rule 12(b)(6) motion to dismiss," courts must "accept all factual allegations in the complaint as true," considering "the complaint in its entirety, as well as other sources courts ordinarily examine when ruling on Rule 12(b)(6) motions to dismiss, in particular, documents incorporated into the complaint by reference, and matters of which a court may take judicial notice." *Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 322 (2007).

First, Kaspersky contends (Br. 40-42) that the allegations made in its complaint are sufficient to withstand a motion to dismiss. Second, it argues (Br. 42-45) that the district court improperly relied on documents in the administrative record in Kaspersky's APA challenge in resolving a motion to dismiss its challenge to Section 1634. Third, Kaspersky contends (Br. 45-47) that the district court incorrectly relied on materials outside the pleadings to establish the truth of the matter asserted, in contravention of the standards governing motions to dismiss. These arguments are wrong.

1. Kaspersky argues that the allegations in its complaint state a claim that Section 1634 is a bill of attainder. Kaspersky emphasizes the assertion in its complaint that Section 1634 singles out the company by name, and that the "statute

imposes impermissible legislative punishment." Br. 41. But whether the statute imposes legislative punishment is a legal, not a factual question. And courts "are not bound to accept as true a legal conclusion" in ruling on motions to dismiss. *Trudeau v. Federal Trade Comm'n*, 456 F.3d 178, 193 (D.C. Cir. 2006). For the reasons provided above, see *supra* pp. 20-27, the district court correctly held that Section 1634 did not impose punishment on Kaspersky, and the district court did not err in declining to accept as true Kaspersky's assertion to the contrary.

2. Kaspersky further argues that the district court committed reversible error by "rely[ing] on the administrative agency record in the APA [challenge to the directive] to decide the government's motion to dismiss the constitutional challenge to congressional action presented in the Bill of Attainder Case." Br. 43. The district court did no such thing. The court consolidated Kaspersky's two suits and resolved them both in a single opinion. See JA 189-90 (describing procedural history); JA 192-214 (resolving Kaspersky's statutory suit); JA 214-23 (resolving Kaspersky's APA suit). Kaspersky principally points to the portion of the district court opinion that merely lays out the background of both suits. Br. 43 (citing JA 173-82). And many of the administrative record citations to which Kaspersky

objects are reproductions of the legislative record leading to the enactment of Section 1634.[10]

Kaspersky suggests (Br. 43) that the district court relied on administrative materials when it summarized (JA 202-03) the considerations that informed Congress's decision to enact Section 1643. But the court's summary simply refers to the "more detail[ed]" background section (JA 202), which not only includes parts of the legislative record reproduced in the administrative record, but also contains direct citations to other key legislative sources.[11] Thus, Kaspersky is simply mistaken

---

[10] Kaspersky identifies as objectionable the district court's reliance in the background section of the opinion on "AR0106, AR0065, AR0557-58, AR0007, [and] AR0011-13." Br. 43. Of those, only the last two citations are to administrative material—the First Manfra Memorandum. The remaining documents are part of the public, legislative record. AR0106 is from a statement for the record of then-Director of National Intelligence James R. Clapper at a Senate hearing. *Worldwide Threat Assessment of the US Intelligence Community: Hearing Before the S. Armed Serv. Comm.* 2 (2015), https://go.usa.gov/xURt5. AR0065 also is from a statement for the record at a Senate hearing. *Worldwide Threat Assessment of the US Intelligence Community: Hearing Before the S. Select Comm. on Intelligence* 1 (May 11, 2017) (statement of Daniel R. Coats, Director of National Intelligence), https://go.usa.gov/xURt7. AR0557-58 is from the House Committee on Science, Space, and Technology. Press Release, *SST Committee Probes Kaspersky Lab In Cabinet Level Request* (July 28, 2017) (discussing *Smith Letter*), https://go.usa.gov/xURtJ.

[11] See JA 175 (quoting from *Disinformation*); *id.* (citing *Bolstering I*); *id.* (citing H.R. Con. Res. 47, 115th Cong. (2017); *id.* (citing *Worldwide Threats*); JA 176 (citing *Bolstering the Government's Cybersecurity: Lessons Learned from Wannacry: Hearing Before H. Comm. on Sci., Space, & Tech.*, 115th Cong. (2017), https://go.usa.gov/xURua); *id.* (citing *Russian Interference in the 2016 U.S. Elections: Hearing Before S. Select Comm. on Intelligence*, 115th Cong. (2017), https://go.usa.gov/xURuB); *id.* (citing *Help or*

in saying that the information outlined in the district court's summary "does not appear in * * * the NDAA legislative record." Br. 44.

The district court fully complied with the applicable standard when it considered that legislative material in ruling on the government's motion to dismiss. See *Tellabs*, 551 U.S. at 322 (courts may consider "matters of which a court may take judicial notice" in deciding a motion to dismiss); *Territory of Alaska v. American Can Co.*, 358 U.S. 224, 226-27 (1959) (courts may "take judicial notice" of "the legislative history of [a] bill").

3. Finally, Kaspersky contends that the district court erred in relying on disputed "material beyond the pleadings" to establish "the truth of the matters asserted." Br. 46, 47. This argument again misunderstands the respective roles of the courts and the political branches. The district court did not weigh evidence in the legislative record to determine whether the federal government's use of Kaspersky software and services in fact presents a national security risk. Rather it considered whether, in light of the information before Congress, it was rational for Congress itself to identify such a risk and to act on that assessment by prohibiting government

---

Hindrance? A Review of SBA's Office of the Chief Information Officer: Hearing Before the H. Comm. on Small Business, 115th Cong. (2017), https://go.usa.gov/xURuV); JA 183 (citing *Bolstering I*) (noting discussion of BOD-17-01); JA 183-84 (citing H.R. Rep. No. 115-376, at 4 (2017)); JA 187-88 (discussing *Executive Summary*).

agencies from using such software and services. See, *e.g.*, JA 203 ("It is not Plaintiffs' or this Court's role to determine *de novo* what precise actions should have been taken in light of this information to protect the nation's cyber-security.").

Kaspersky identifies only two instances (Br. 46-47) in which it claims the district court relied on a document from the administrative record to establish the truth of a matter relevant to the court's consideration of Section 1634. In one instance, the district court explained that, because congressional committees had held hearings on DHS's issuance of the directive, it was reasonable to infer that Congress, like DHS, was motivated to "stem the risk of Russian cyber-attacks." Br. 46 (quoting JA 212 (in turn citing JA 49 (Decision of the Acting Sec'y))). It is odd for Kaspersky to object to that inference, however, as Kaspersky's own complaint alleges that Congress was motivated by the "threat" of "Kremlin hack[ing]" in prohibiting the use of Kaspersky software and services on federal information systems. JA 144 ¶ 28 (quoting from Shaheen Opinion); see *id.* ("That threat is posed by antivirus and security software products created by Kaspersky Lab.") (quoting from Shaheen Opinion). In any event, that motivation is evident in the legislative material. See, *e.g.*, *Smith Letter* 1, https://go.usa.gov/xU5xR (expressing "concern[] that Kaspersky Lab is susceptible to manipulation by the Russian government, and that its products could be used as a tool for espionage, sabotage, or other nefarious acts against the United States").

The second instance is the district court's reference (JA 206) to the Second Manfra Memorandum's explanation (JA 74) of the information-security risks uniquely presented by Kaspersky products. The district court pointed to that explanation as a basis for concluding that Congress could reasonably take immediate action addressing Kaspersky but not other cybersecurity vendors. JA 206. Assistant Secretary Manfra presented this rationale in her committee testimony. See *Bolstering II*, at 22, https://go.usa.gov/xU5CA. And, in any event, that information is also contained elsewhere in the legislative material that supported Congress's enactment of Section 1634. See, *e.g.*, *Bolstering I*, at 48-49, https://go.usa.gov/xU5ad (Kanuck Statement) (providing testimony about some of the factors that make Kaspersky "more prone or susceptible" to misuse by the Russian government "than other cyber security vendors"). Moreover, the district court addressed this point only in rejecting Kaspersky's argument that the specificity of Section 1634 alone demonstrates that the provision is punitive. JA 205. But Kaspersky now concedes that "[s]pecificity alone does not render a statute an unlawful bill of attainder." Br. 15.

II. KASPERSKY'S CHALLENGE TO THE DIRECTIVE IS NON-JUSTICIABLE

"[T]he irreducible constitutional minimum of standing contains three elements." *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992). First, a plaintiff must have suffered "an injury in fact—an invasion of a legally protected interest

which is (a) concrete and particularized, and (b) actual or imminent, not conjectural or hypothetical." *Id.* (citations and quotation marks omitted). Second, the plaintiff's alleged injury must be causally connected to the challenged action of the defendant. *Id.* And third, "it must be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." *Id.* (quotation marks omitted). Courts must "assess standing as of the time a suit is filed." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 426 (2013). And the plaintiff's personal interest must continue through the existence of the suit, or the suit becomes moot. *United States Parole Comm'n v. Geraghty*, 445 U.S. 388, 397 (1980).

A favorable decision on Kaspersky's challenge to the directive would not remedy Kaspersky's alleged injuries because those injuries are traceable to Section 1634. See *Branton v. Federal Commc'ns Comm'n*, 993 F.2d 906, 910 (D.C. Cir. 1993) ("[The causation and redressability] requirements tend to merge * * * in a case such as this where the requested relief consists solely of the reversal or discontinuation of the challenged action."). The district court therefore properly dismissed Kaspersky's challenge to the directive for lack of jurisdiction.

A. A Favorable Decision Concerning the Directive Would Not Redress Kaspersky's Alleged Injuries

This Court has held that courts may (and in some cases must) sequence the order of issues decided, resolving threshold issues that are "logically antecedent to

the merits" of a plaintiff's claim before proceeding to the merits. *Vila v. Inter-American Inv. Corp.*, 570 F.3d 274, 283 (D.C. Cir. 2009) (exercising pendent jurisdiction to decide "threshold" statute-of-limitations issue); see *Western Md. Ry. v. Harbor Ins. Co.*, 910 F.2d 960, 962-63 (D.C. Cir. 1990) ("[A district] court need only decide whether an absent party is indispensable if it determines that the party's joinder is infeasible, and it need only decide whether joinder is feasible if it decides that an absentee's presence is necessary.") (discussing Fed. R. Civ. P. 19).

In light of Section 1634, Kaspersky could obtain no redress from a favorable decision in its challenge to the directive. The prohibition in Section 1634 is broader than that in the directive and fully includes the prohibition in the directive, as the district court concluded and as Kaspersky has conceded. JA 187; Kaspersky Emergency Inj. Mot. 5, 19. The constitutionality of the statute is therefore "logically antecedent" to Kaspersky's challenge to the directive. Having upheld the validity of the statute, the district court properly considered the effect of that ruling on Kaspersky's challenge to the directive. And the district court correctly concluded that Kaspersky lacks sufficient personal interest to challenge the directive, rendering Kaspersky's claims nonjusticiable, because a favorable decision concerning the directive would do nothing to ameliorate the larger injury to Kaspersky caused by the statute. See, *e.g.*, *Physician's Educ. Network, Inc. v. Department of Health, Educ. & Welfare*, 653 F.2d 621, 623-24 (D.C. Cir. 1981) (plaintiffs lacked standing to

challenge agency report on procedural grounds, where, while case was on appeal, Congress enacted legislation adopting recommendations made in report). Thus, whether as a matter of standing or mootness, Kaspersky's challenge to the directive is not justiciable. *Garden State Broad. Ltd. v. Federal Commc'ns Comm'n*, 996 F.2d 386, 394 (D.C. Cir. 1993) ("The requisite personal interest that must exist at the commencement of the litigation (standing) must continue throughout its existence (mootness)."); *Foretich*, 351 F.3d at 1210 (same).

It does not matter that Section 1634's prohibition will become effective on October 1, 2018, and so was not in effect when Kaspersky filed suit. See NDAA § 1634(b). October 1 is a deadline by which federal entities must ensure their compliance with the prohibition. To meet that deadline, federal entities would immediately refrain from purchasing Kaspersky products because "any new investment in Kaspersky software would frustrate agency efforts to bring their information systems in compliance with the NDAA." JA 135 (Declaration of Grant Schneider, Acting Fed. Chief Info. Sec. Officer, Office of Mgm't &Budget); see *id.* at 134 ("Acquiring Kaspersky software only to remove it months later (i.e., by October 1, 2018) would be costly, inefficient, and inexcusably wasteful."); see generally *Land v. Dollar*, 330 U.S. 731, 734 n.4 (1947) ("[W]hen a question of the District Court's jurisdiction is raised, * * * the court may inquire by affidavits or otherwise, into the facts as they exist.").

B. Kaspersky's Challenge to the Directive Fails to State a Claim

In any event, Kaspersky failed to state a procedural due-process claim on which relief can be granted, an alternative ground on which this Court may affirm. See *Parsi v. Daioleslam*, 778 F.3d 116, 126 (D.C. Cir. 2015) ("Ordinarily, a court of appeals can affirm a district court judgment on any basis supported by the record, even if different from the grounds the district court cited."). Procedural "due process is flexible and calls for such procedural protections as the particular situation demands." *National Council of Resistance of Iran v. Department of State*, 251 F.3d 192, 205 (D.C. Cir. 2001). "Due process ordinarily requires that procedures provide notice of the proposed official action and the opportunity to be heard at a meaningful time and in a meaningful manner." *Ralls Corp. v. Committee on Foreign Inv. in the U.S.*, 758 F.3d 296, 318 (D.C. Cir. 2014) (quotation marks omitted). Most critically, "the right to know the factual basis for the action and the opportunity to rebut the evidence supporting that action are essential components of due process." *Id.* Those components were part of the administrative remedy provided here, which satisfied the constitutional requirement.

In this case, DHS issued the directive on September 13, 2017. The directive required federal agencies to "begin to implement" agency plans to remove Kaspersky-branded products from their information systems ninety calendar days after the issuance of the directive, "unless directed otherwise by DHS based on new

information." 82 Fed. Reg. at 43,783; Add. 5. The ninety-day period before the removal requirement became effective gave Kaspersky and any other entities whose commercial interests are affected by the directive an opportunity to respond, and gave DHS an opportunity to consider any submissions in deciding whether to modify the directive.

Under the administrative process DHS established, responses were due by November 3, 2017, which was forty-five days after the publication of the federal register notice. 82 Fed. Reg. at 43,784; Add 6. Affected entities were given the opportunity to provide "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." *Id.* The same day DHS issued the directive, it sent a letter to Eugene Kaspersky informing him of the issuance of the directive and the administrative review process and enclosing the Acting Secretary's decision memorandum. JA 183; see JA 58 (noting that decision memorandum was sent to Kaspersky); JA 48-52 (Decision of the Acting Sec'y). Moreover, DHS later sent Kaspersky's counsel the First Manfra Memorandum, with exhibits, "to ensure that Kaspersky had the complete unclassified rationale for issuance of [the directive]." JA 58 (Second Manfra Mem.).

Kaspersky "submitted a lengthy response" to the directive. JA 184; see generally *id.* (describing response). In addition, Kaspersky and its "counsel met with

DHS officials to discuss" the directive. JA 184. The meeting included discussion of Kaspersky's written submission, and Kaspersky responded to DHS's questions. JA 184-85. On December 4, 2017, Assistant Secretary Manfra issued a second memorandum, which included a detailed discussion of Kaspersky's submission and the reasons why the submission did not mitigate the risks identified by DHS. JA 56-80; see JA 61-79; see *supra* pp. 7-8 (detailing Kaspersky submission). Assistant Secretary Manfra therefore recommended that the Acting Secretary maintain the directive without modification. JA 79-80. The Acting Secretary accepted that recommendation and issued a final decision on December 6, 2017. JA 126-29.

The administrative process thus gave Kaspersky advance notice of DHS's planned prohibition of Kaspersky-branded products on federal agency information services. That notice informed Kaspersky of the factual basis for DHS's decision, and it gave Kaspersky an opportunity to respond before DHS determined whether to rescind, modify, or maintain the directive. That is all procedural due process requires, and it is no less than what this Court has held is required in other cases involving the government's response to national security risks. See, *e.g.*, *Ralls*, 758 F.3d at 318 (in a national security case, due process requiring providing affected entity with "notice of the proposed" action, "access to the unclassified evidence supporting the designation and an opportunity to rebut that evidence"); see also *Holy Land Found. for Relief & Dev. v. Ashcroft*, 333 F.3d 156, 163 (D.C. Cir. 2003)

(predeprivation notice not required upon an adequate showing that earlier notice "would impinge upon the security and other foreign policy goals of the United States").

C. Kaspersky's Contrary Arguments Lack Merit

Kaspersky argues that the district court erred in dismissing its challenge to the directive because (1) at the time DHS issued the directive, Kaspersky suffered immediate injury; (2) invalidating the directive would have addressed some of Kaspersky's injuries, even if not fully; and (3) the district court's decision to uphold the validity of Section 1634 is erroneous. All of these arguments are flawed.

For standing purposes, a court's focus is not on the time of the challenged action but on the time when suit is brought. *Entergy Servs., Inc. v. Federal Energy Regulatory Comm'n*, 391 F.3d 1240, 1245 (D.C. Cir. 2004) ("Standing is assessed at the time the action commences, *i.e.*, in this case, at the time [Petitioner] sought relief from an Article III court.") (quotation marks omitted; alteration in original). There is a significant question whether Kaspersky had standing at the time it brought its first suit, which did not challenge the then-recent enactment of Section 1634. But the Court need not address that issue, because, as discussed above, see *supra* pp. 47-49, the validity of Section 1634 makes Kaspersky's challenge to the directive nonjusticiable.

Kaspersky seeks to avoid that conclusion by arguing that invalidating the directive would remedy some, even if not all, of Kaspersky's alleged injuries. Br. 51. But because Section 1634 is broader than the directive and includes all of the latter's prohibitions, the invalidation of the directive on procedural due-process grounds would not remedy any of Kaspersky's alleged economic and reputational injuries. Kaspersky offers no concrete explanation of how such a ruling would redress its injuries, and instead makes only unsupported, speculative assertions that it would do so. *Id.* That is not sufficient to establish the district court's jurisdiction over Kaspersky's challenge to the directive.

Finally, the district court correctly rejected Kaspersky's challenge to Section 1634 on the merits, for the reasons provided above.[12]

[12] Kaspersky further argues (Br. 52-53) that, for redressability purposes, a party asserting a constitutionally defective process need not demonstrate that a constitutionally proper process would have led to a different substantive result. There is no need for this Court to reach that issue.

CONCLUSION

The Court should affirm the district court's judgment.

Respectfully submitted,

CHAD A. READLER
Acting Assistant Attorney General

H. THOMAS BYRON III
LEWIS S. YELIN
Attorneys, Appellate Staff
Civil Division, Room 7239
U.S. Department of Justice
950 Pennsylvania Ave., NW
Washington, DC 20530
(202) 514-3425

July 30, 2018

ADDENDUM

ADDENDUM CONTENTS

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.

CERTIFICATE OF COMPLIANCE

I hereby certify that this brief complies with the requirements of Fed. R.. P. 32(a)(5) and (6) because it has been prepared in 14-point Goudy Old Style, a proportionally spaced font.

I further certify that this brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because it contains 12,532 words, excluding the parts of the brief exempted under Rule 32(f) and D.C. Circuit Rule 32(e)(1), according to the count of Microsoft Word.

s/ Lewis S. Yelin
LEWIS S. YELIN
Counsel for Appellees

CERTIFICATE OF SERVICE

I hereby certify that on July 30, 2018, I electronically filed the foregoing brief with the Clerk of the Court for the United States Court of Appeals for the District of Columbia Circuit by using the appellate CM/ECF system, which, under the Court's rules, constitutes service on all parties registered with the CM/ECF system.

I further certify that I caused eight paper copies of this brief to be filed with the Court.

s/ Lewis S. Yelin
LEWIS S. YELIN
Counsel for Appellees