UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

KASPERSKY LAB, INC.; and KASPERSKY LABS LIMITED,	)	
Plaintiffs,	)	
v.	)	Civ. No. 17-2697 (CKK)
U.S. DEPARTMENT OF HOMELAND SECURITY; and KIRSTJEN NIELSEN *Secretary of Homeland Security*	)	
Defendants.	)	

MEMORANDUM IN OPPOSITION TO PLAINTIFFS' MOTION FOR SUMMARY JUDGMENT AND IN SUPPORT OF DEFENDANTS' MOTION TO DISMISS OR, IN THE ALTERNATIVE, FOR SUMMARY JUDGMENT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

RULES

REGULATIONS

OTHER AUTHORITIES

INTRODUCTION

The U.S. 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 cyber threats. To this end, Congress has vested the Secretary of Homeland Security with broad authority to take actions she deems appropriate to protect federal information systems against cyber intrusion. Among the tools Congress gave the Secretary is the Binding Operational Directive (BOD), a compulsory direction to federal agencies to take specific actions in response to a "known or reasonably suspected information security threat, vulnerability, or risk." 44 U.S.C. §§ 3552(b)(1), 3553(b)(2). The Secretary exercises this authority by making predictive judgments, often based on sensitive intelligence reporting, about whether a particular threat or vulnerability is serious enough to warrant a government-wide response.

This past September, the Acting Secretary issued a BOD directing federal agencies to take a series of actions concerning Kaspersky software on their information systems. Agencies were to gather information about the software, develop plans to remove it, and, unless directed otherwise in 90 days, begin removal. The action was not taken lightly. The BOD was issued only after extensive investigation and consultation with cybersecurity experts inside and outside the Department of Homeland Security (DHS or the Department), and it was paired with an administrative process that afforded Kaspersky the complete unclassified rationale for the Acting Secretary's decision and an opportunity to respond to her concerns before the day-90 removal requirement. Those concerns, reduced to their essence, were that Russia, on its own or in collaboration with Kaspersky, could use Kaspersky software installed on U.S. government information systems as an entry point for espionage or hostile cyber activities. Russia is a sophisticated adversary that is constantly probing opportunities to compromise and exploit access

to U.S. networks. Its intelligence services have an unusually close relationship with Kaspersky and virtually unbounded authority under Russian law to compel access to information stored on the company's Russian servers and to intercept data transmissions between the company and its U.S. customers. As long as Kaspersky's products are on U.S. government networks, Russia will have the ability to exploit Kaspersky's access for hostile purposes, with or without the company's cooperation. That was a risk the Acting Secretary could not accept.

Kaspersky Lab, Inc. and its affiliate, Kaspersky Labs Ltd. (collectively, Kaspersky), have brought this action seeking to overturn the BOD. Kaspersky claims DHS deprived it of constitutional due process by effectively excluding the company from federal business without providing it with adequate notice and opportunity to be heard, and violated the Administrative Procedures Act (APA) by failing to offer sufficient evidence in support of its decision. Kaspersky's claims for relief are addressed only to the BOD, despite the fact that the BOD's prohibition was codified and expanded by Congress in the National Defense Authorization Act for Fiscal Year 2018 (NDAA). The NDAA imposes a comprehensive, government-wide ban on the use of Kaspersky hardware, software, and services, thereby requiring agencies, by October 1 of this year, to remove *any* product containing Kaspersky software (not only the "Kaspersky-branded" products covered by the BOD) found on *any* information system (not only the non-national security systems covered by the BOD). But even though the NDAA's ban proscribes the same conduct as the BOD (and more), and for the same reason, Kaspersky does not seek relief from the statute's prohibition in this case, having elected to challenge it in a separate action.

As a threshold matter, Kaspersky lacks standing to sue because a ruling in its favor would not redress its complained-of harms. The D.C. Circuit has long held that where two laws—here, the BOD and the NDAA's ban—independently produce the same alleged harm, a judicial decree

overturning just one does not satisfy the redressability requirement for standing. Rescinding the BOD would leave the NDAA ban in place, which means agencies still would be required to remove and stop using Kaspersky products, and there still would be law branding the company's software as a security risk. Nothing of practical value would come from a favorable ruling, and whatever value Kaspersky attaches to the prospect of being legally permitted to sell software to the U.S. government during the brief period between the rescission of the BOD and the date the NDAA's categorical ban kicks in (October of this year) does not amount to a redressable Article III injury.

Kaspersky's new lawsuit challenging the NDAA ban does not cure the standing defect that existed when this action was filed. Standing is determined based on the circumstances existing when the complaint is filed, and may not be based on post-filing developments, including new lawsuits. Although Kaspersky's challenge to the NDAA ban has been temporarily consolidated with this case, the consolidation is for the limited purpose of briefing; the two cases have not been merged. Instead, they will retain their separate identities, and the NDAA challenge will remain, like any other post-filing development, irrelevant to Kaspersky's standing to challenge the BOD. But even if the Court could consider it, the mere existence of a challenge to the NDAA ban hardly supports an inference that the statute is in jeopardy. Indeed, as the government will show in the NDAA suit, Kaspersky's challenge to the NDAA ban should not survive the pleadings stage.

Kaspersky's claims also fail on the merits. The company cannot prevail on its claim that DHS denied it due process. Kaspersky exaggerates the process to which it was constitutionally entitled and undervalues the process it actually received. Kaspersky's own account shows that DHS went above and beyond what is procedurally required, including providing the company with a highly detailed, 20-plus page internal memorandum, with 47 exhibits, explaining the unclassified rationale for issuing the BOD; and allowing it 52 days to submit a response, along with any

mitigation proposals, which DHS examined closely (as evidenced by the additional 25-page December 4 memorandum to the Acting Secretary at AR 752-776), before it made a final decision. Kaspersky says it was denied "pre-deprivation process," but that claim rests on the erroneous view that the company was entitled to administrative process before DHS issued the BOD – that is, before DHS took an *initial* action, which, were it to remain unchanged, could affect its legal rights.

The company's APA claim fares no better. Kaspersky is not the first litigant to attempt to use the APA to police a federal agency's actions under the Federal Information Security Modernization Act of 2014 (FISMA) or its similar predecessor statute, the Federal Information Security Management Act of 2002 (FISMA 2002). Since FISMA 2002's enactment, multiple plaintiffs have brought APA challenges seeking to enjoin agency decisions under the statute. Not one of these suits has prevailed, and every court to consider the issue has agreed that decisions under these statutes are committed to agency discretion and thus outside the scope of APA review. There is no reason why Kaspersky's APA challenge should be any different. The wide discretion vested in the Secretary to exercise the BOD authority, together with the absence of any judicial standards to test her judgment, puts this case directly in line with the other FISMA and FISMA 2002 precedents.

Even if APA review were appropriate, the unclassified record amply supports DHS's determination that Kaspersky software presents known and reasonably suspected risks to federal information and information systems. The Acting Secretary's decision was informed by recommendations from DHS's top cybersecurity officials, including hundreds of pages of evidence and written analysis documenting the pernicious and rapidly evolving nature of the Russian cyber threat, the chilling prospect of Russian agents or Kaspersky using antivirus software running on federal networks as a platform for malicious cyber operations, and the reasons why Kaspersky software poses an intolerably high risk of falling under Russian control. Those judgments, which

are largely uncontroverted at summary judgment, are entitled to deference, and easily satisfy the APA's requirement that DHS's action be supported by substantial evidence and demonstrate a rational connection to the underlying facts.

For these reasons, this Court should dismiss this suit for lack of jurisdiction or, alternatively, deny Kaspersky's motion for summary judgment and grant the government's cross-motion.

STATUTORY BACKGROUND

FISMA is the main statute establishing authorities and responsibilities for federal agency information security. 44 U.S.C. §§ 3551-3558. Under FISMA, each agency must develop and implement its own plans for protecting the security of the information and systems that support its operations. Those efforts are jointly overseen by DHS and the Office of Management and Budget (OMB). Under this division of labor, OMB develops and oversees the implementation of government-wide information security policies, principles, standards, and guidelines; DHS, in consultation with OMB, is responsible for administering the implementation of agency information security policies and practices, including by assisting OMB in carrying out its authorities as well as monitoring agencies' implementation of their information security policies and practices and providing them with operational and technical assistance as they implement the policies, principles, standards, and guidelines developed by OMB. *See* 44 U.S.C. §§ 3553(a), (b).

Congress authorized the Secretary of DHS to issue compulsory direction to agencies, or a "Binding Operational Directive (BOD)," "for purposes of safeguarding Federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk." *Id.* §§ 3552(b)(1), 3553(b)(2). The Secretary can use BODs to address a range of information security risks, including "requirements for the mitigation of exigent risks to information systems," and "other operational requirements as the Director [of OMB] or Secretary,

in consultation with the Director, may determine necessary." *Id*. § 3553(b)(2). BODs may be revised or repealed by OMB if found to be inconsistent with OMB-issued policies or principles, *id*. § 3552(b)(1), but as long as they comply with that requirement and satisfy the statutory definition, the Secretary has complete discretion to determine when to issue them.

FACTUAL BACKGROUND

I. Kaspersky's Software and Connections to Russia

When an enterprise (in this case, an agency) installs Kaspersky's antivirus software and consents to the license agreement, it gives the software high-level privileges and broad access to files on the information system on which it is installed. The enterprise also agrees to let Kaspersky update the software, and to transfer certain data back to servers located in (or accessible from) Russia for further evaluation. AR 755, 761-62. For an enterprise that participates in the Kaspersky Security Network (KSN), the list of data it consents to be automatically transferred is especially expansive and sensitive. AR 762-63, 8-9, 29-30.

Most of these features are common to commercial antivirus software and necessary to perform its function. For example, antivirus software needs unfettered file access to scan for malicious code, AR 7-8, and updates are critical to ensure the software keeps apace with new and evolving threats. But the same powerful features and elevated privileges that make antivirus software effective make it a tempting attack platform for intelligence services and dangerous if its access and privileges are exploited for malicious purposes.

The presence of Kaspersky antivirus products on U.S. government networks presents a significant risk that the Russian government will exploit Kaspersky's access and gravely compromise our nation's security. For example, Russian agents could install malicious code under the guise of a security update (affecting the confidentiality, integrity, or availability of government

information or information systems), or simply decline to install security updates that are actually needed. AR 30, 763. They also could extract virtually any file of interest under the pretext that it needs to be inspected for malware. AR 8-9.

Concerns about exploitation stem in part from Kaspersky's close ties to the Russian military and intelligence services. Kaspersky holds licenses and has other connections with the Russian Federal Security Service (FSB) that reflect an unusually close relationship with the government, beyond that of an ordinary regulated entity. AR 764-65, 767-68, 11-13. Kaspersky and the FSB are publicly reported to have collaborated on a software-development project, and their respective technicians work side-by-side on FSB investigations. AR 764-65, 12-13, 566. Eugene Kaspersky, the company's founder and CEO, spent years working for the Ministry of Defense, after graduating from an engineering school overseen by the KGB. AR 764, 12. He maintains various personal and professional ties with the Russian government, and has assembled a leadership team with a similar pedigree. The firm's Chief Operating Officer is a former lieutenant-colonel in the Russian military, and its top lawyer, the official presumably responsible for ensuring that the Russian government does not overstep its legal boundaries, is ex-KGB. AR 764, 13.

The prospect that Kaspersky would be willing to facilitate a Russian cyberattack is not the only concern. Russia has the means to use Kaspersky software as a platform for espionage whether or not the company is willing to cooperate. For example, Russian law requires the FSB to carry out its intelligence and other activities in collaboration with private firms in Russia, and the private firms are legally obligated to assist the FSB in the execution of FSB intelligence, counterintelligence, and other duties. AR 780-81. This could include requiring that Kaspersky give the FSB access to U.S. government user data. AR 15, 766-67, 782-88. The FSB also is authorized to second personnel to private enterprises, with the head of the enterprise's consent, and with the

FSB personnel remaining in FSB military service during the secondment. AR 14, 781-82. Further, companies like Kaspersky can be required to install equipment or software that enables the FSB to monitor data transmissions between the company and its users, AR 767, 789-93, 14-15.

More broadly, the U.S. Intelligence Community has painted a stark picture of the Russian cyber threat. The Director of National Intelligence has described Russia as a "full-scope cyber actor that will remain a major threat to the U.S. Government." Moscow has a "highly advanced offensive cyber program," and recently has "assumed a more aggressive cyber posture," as shown by its multi-faceted campaign to influence the 2016 U.S. election as well as numerous destructive and costly attacks outside the United States. AR 9-10, 65. Russian intelligence services will continue to "develop capabilities to provide Putin with options to use against the United States," and Russian cyber operations will continue to target the United States, whether to collect intelligence, conduct influence operations, or "prepare the cyber environment for future contingencies." AR 65.

II. Kaspersky Comes under Public Scrutiny

DHS was not the first U.S. agency to act on concerns about the presence of Kaspersky software on federal networks, and it certainly was not the first to call public attention to the issue. Suspicions about Kaspersky's ties to the Kremlin have been mounting for years,[1] and scrutiny from lawmakers and intelligence officials only intensified after Russian intelligence services orchestrated cyberattacks against the United Stated in connection with the 2016 elections.

An early signal that the company was under scrutiny came in March 2017, during a Senate hearing on Russian cyber activities. Citing a "long history" of open-source reporting connecting Kaspersky to Russian security services, Senator Marco Rubio asked a panel of cybersecurity

[1] *See, e.g.*, *Russia's Top Cyber Sleuth Foils US Spies, Helps Kremlin Pals*, Wired (July 23, 2012) (Singer Decl., Ex. 3-A)

experts if they would feel comfortable using Kaspersky products on their own devices.[2] The following month, the U.S. Senate Select Committee on Intelligence reportedly asked the Director of National Intelligence and the Attorney General to investigate the company's ties to the Russian government,[3] and two House members introduced a bill describing Kaspersky as "a company suspected of having ties with the Russian intelligence services and later caught up in a Russian espionage investigation."[4] In May, six U.S. intelligence directors, including the directors of the Central Intelligence Agency and the National Security Agency, told the Senate Intelligence Committee that they would not be comfortable using Kaspersky products on their computers. NSA Director Rogers said he was "personally involved" in monitoring the Kaspersky issue, and CIA Director Pompeo acknowledged that concerns about Kaspersky products "ha[d] risen to the director" level at CIA.[5] Throughout the summer of 2017, lawmakers continued to raise questions about Kaspersky—first during a House Science hearing on the lessons learned from the WannaCry attacks,[6] then during a Senate Intelligence Committee hearing on Russian interference in the 2016 elections,[7] and again during a July hearing before the House Committee on Small Business.[8]

---

[2] *Disinformation: A Primer in Russian Active Measures and Influence Campaigns, Panel II*, 115th Cong. 40 (March 30, 2017), (Singer Decl., Ex. 3-B)

[3] *See Bolstering the Government's Cybersecurity: Assessing the Risks of Kaspersky Lab Products to the Federal Government*, H. Comm. on Science, Space, and Technology, 115th Cong. (2017), (Singer Decl., Ex. 3-C)

[4] H.R. Con. Res. 47, 115th Cong. (2017), (Singer Decl., Ex. 3-D)

[5] *Hearing on Worldwide Threats Before the S. Select Comm. on Intelligence*, 115th Cong. (May 11, 2017), https://www.intelligence.senate.gov/hearings/open-hearing-worldwide-threats-hearing-0

[6] *Bolstering the Government's Cybersecurity: Lessons Learned from Wannacry*, 115th Cong. (June 15, 2017) (Singer Decl., Ex. 3-E)

[7] *Russian Interference in 2016 U.S. Elections*, 115th Cong. (June 21, 2017) (Singer Decl, Ex. 3-F)

[8] *Help or Hindrance? A Review of SBA's Office of the Chief Information Officer*, 115th Cong. (July 12, 2017) (Singer Decl., Ex. 3-G)

In the ensuing months, lawmakers and regulators began taking more concrete steps to address concerns about Kaspersky software. In June, Senator Tom Cotton proposed an amendment to an Iran sanctions bill that called for the imposition of economic sanctions against Kaspersky employees in Russia.[9] In July, the Senate version of the NDAA was introduced with a provision barring the use of Kaspersky software on Department of Defense (DOD) information systems.[10] Senator Jeanne Shaheen later filed an amendment to the House version of the NDAA to prohibit the use of Kaspersky software government-wide.[11] In support of the amendment, the Senator cited "alarming and well-documented" ties between Kaspersky and the Kremlin.[12] Around this time, Representative Lamar Smith, Chairman of the House Committee on Science, Space, and Technology, sent a letter to various federal agencies requesting information about their use of Kaspersky software and expressing concern that the company "is susceptible to manipulation by the Russian government." AR 557-58. Also in July 2017, the General Services Administration (GSA) removed Kaspersky from the agency's lists of pre-approved vendors for contracts that cover information technology products and services and digital photographic equipment. AR 559-61. GSA said the action was taken "after review and careful consideration," consistent with its priority "to ensure the integrity and security of U.S. government systems and networks." *Id*.

In the meantime, Kaspersky's connections to the Kremlin had attracted extraordinary publicity. While the bulk of these reports focused on increasing scrutiny from the U.S. government, a number of stories purported to bring new information to light, including a July 2017 Bloomberg report that

[9] 163 Cong. Rec. S3492 (2017) (Singer Decl., Ex. 3-H)

[10] S. 1519, 115th Cong. (2017) (Singer Decl., Ex. 3-I)

[11] Amendment (SA 663) to H.R. 2810, 115th Cong. (2017) (Singer Decl., Ex. 3-J)

[12] Senator Jeanne Shaheen's Legislation to Ban Kaspersky Software Government-Wide Passes Senate As Part of Annual Defense Bill (Sept. 18, 2017) (Singer Decl., Ex. 3-K)

Kaspersky has a much closer relationship to Russian intelligence services than the company had previously admitted.[13] These reports added to a steady drumbeat of negative publicity that only continued with the September 8, 2017 news that Best Buy, the nation's largest consumer electronics retailer, was halting sales of Kaspersky products, with sources familiar with the decision attributing it to concerns over the company's ties to Russian intelligence services.[14]

III. The Binding Operational Directive

It was against this backdrop that DHS, on September 13, 2017, issued BOD 17-01. Invoking her authority under FISMA, Acting Secretary Elaine Duke issued the directive after determining that the presence of Kaspersky products on federal information systems presents a "known or reasonably suspected threat, vulnerability, or risk" to federal information and information systems. AR 628, 631. The BOD directed federal agencies to identify any use of Kaspersky-branded products within 30 days, provide a plan to remove them within 60 days, and, unless directed otherwise by DHS based on information it learned during the administrative review period, to begin removing the products at 90 days. AR 634-35.

In the weeks and months before the BOD, the Department engaged in extensive consultations with its cybersecurity experts and interagency partners and reviewed information from a variety of sources, including classified intelligence reports. But while the Acting Secretary considered both classified and unclassified information, she has emphasized that her decision to issue the BOD is justified on the strength of the unclassified evidence alone.[15] AR 631. That decision, the

[13] Cyrus Farviar, *Kaspersky under scrutiny after Bloomberg story claims close links to FSB*, Arts Technica (July 11, 2017) (Singer Decl., Ex. 3-L)

[14] Reuters Staff, *Best Buy stops sale of Russia-based Kaspersky products*, Reuters (Sept. 8, 2017) (Singer Decl., Ex. 3-M)

[15] The classified materials considered by the Acting Secretary have been compiled in a classified annex to the administrative record. The classified material does, of course, further support the

Acting Secretary explained in a memo released with the BOD, is based on three principal concerns: (1) the broad access to files and elevated privileges provided by antivirus products and services, including Kaspersky products, that can be exploited by malicious cyber actors to compromise information systems; (2) the ties between certain Kaspersky officials and Russian intelligence and other government agencies; and (3) Russian legal provisions that allow Russian intelligence agencies to request or compel assistance from Kaspersky and to intercept communications transiting Russian networks. AR 629, 753-54.

The Acting Secretary's decision is supported by a robust administrative record totaling hundreds of pages of source exhibits and an additional hundred-plus pages of written analysis. These materials include two evidentiary memoranda prepared by DHS's chief cybersecurity official, the Assistant Secretary for Cybersecurity and Communications. AR 3-23, 752-76. The Assistant Secretary, in turn, relied on research and analysis from cybersecurity experts in the Department's National Protection and Programs Directorate, including two risk assessments prepared by the National Cybersecurity and Communications Integration Center (NCCIC) (AR 25-32, 822-32), as well as a report on relevant aspects of Russian law (AR 777-821).

DHS provided an administrative process to Kaspersky and any other entity that claimed its commercial interests would be directly impacted by the BOD. AR 637-38, 639-46. The administrative process was designed to ensure that Kaspersky and other parties would have a

---

Acting Secretary's decision, and DHS accordingly does not waive any argument that national security information may ultimately be necessary to adjudicate some or all of Kaspersky's claims. Rather, DHS believes that the BOD can be sustained on the basis of the unclassified portions of the administrative record. Should the Court conclude that the unclassified portions of the administrative record are not sufficient, however, the parties and the Court may need to confront further questions about the impact of national security information on this proceeding. By deferring such questions until the parties have endeavored to litigate on the basis of *unclassified* information, the Court can meaningfully adjudicate Kaspersky's claims without DHS and the Court needing to address the impact of national security information on this case.

reasonable amount of time to prepare a response, leaving the Acting Secretary with the remaining time to consider and respond to any information submitted before reaching a final decision at the 90-day mark. This feature of the process was spelled out in various documents, including the BOD, which stated that the 90-day start of removal applies "unless directed otherwise by DHS based on new information," AR 635; the Decision to issue the BOD, which stated that DHS "reserves the right to modify or terminate the BOD based on new information provided during the administrative process," AR 630; and a September 13, 2017 letter to Eugene Kaspersky, which highlighted Kaspersky's ability to address the grounds for the decision as "an important element" of the Secretary's decision on whether to modify or terminate the requirement to start removal on day 90, AR 637. On September 19, 2017, DHS published a Federal Register Notice detailing the administrative process available to Kaspersky and any other directly impacted parties. Kaspersky was given 45 days from the notice in the Federal Register (plus a one-week extension granted by DHS upon the request of Kaspersky's counsel) to come forward with information to address DHS's concerns. Kaspersky made its submission on November 10, 2017. AR 647-751.

Over the ensuing weeks, DHS engaged in a fully interactive process with Kaspersky. It closely considered the company's submission of information in opposition to the BOD and participated in an ongoing dialogue with Kaspersky's lawyers, including an in-person meeting. AR 754-55. After closely reviewing the company's submission, as well as additional information obtained during the review period, the Acting Secretary exercised her discretionary authority under FISMA and ultimately made a risk assessment: the presence of Kaspersky's products on federal information systems creates a "known" and "reasonably suspected" risk that the Russian government, acting with or without Kaspersky's consent or assistance, will exploit the access provided by these

products for purposes contrary to U.S. national security. AR 935-937. The Acting Secretary therefore determined that the BOD should be maintained without modification.

Consistent with the BOD, all federal executive branch agencies have reported to DHS on whether they identified Kaspersky-branded products on their federal information systems. AR 755. Based on agency reports in response to the BOD and other communications between DHS and the agencies, DHS gained information about, among other matters, the types of Kaspersky products deployed on federal networks, the types of Kaspersky services provided to federal customers, the types of devices that Kaspersky products protect, and the use of Kaspersky products by government contractors. AR 755-756. In total, fourteen agencies identified Kaspersky-branded products on their information systems. AR 756. Although the BOD's requirement to begin removal did not take effect until day 90, and even then only if agencies had not been directed otherwise, some agencies removed the software ahead of day 90. *Id*. These agencies acted on their own, in accordance with standard agency risk-management responsibilities under FISMA. *Id*. DHS did not advise these agencies to start removal before day 90. *Id*.

IV. The National Defense Authorization Act of 2018

On December 12, 2017, the President signed the NDAA into law. Section 1634 prohibits federal agencies from using "any hardware, software, or services developed or provided, in whole or in part, by [Kaspersky]." Section 1634(a) enacts a comprehensive ban on Kaspersky products that exceeds the scope of the BOD in two important respects. First, while the BOD does not apply to national security systems or other systems used by DOD and the Intelligence Community, 44 U.S.C. § 3553(b), (d), (e), the NDAA ban applies government-wide. Second, while the BOD exempts two specific Kaspersky-branded services and does not apply to Kaspersky code embedded in the products of other companies, the NDAA ban covers all agency use of Kaspersky hardware,

software, and services, whether of branded Kaspersky products or Kaspersky code embedded in software or hardware products sold by third-party vendors.

Section 1634(a) requires that all agencies discontinue use of Kaspersky products and services by October 1, 2018, the first day of the new fiscal year. In the meantime, Congress directed DOD, 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 submit a report to Congress addressing a host of topics, including the "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." *Id.* § 1634(c)(2).

DISCUSSION

I. Kaspersky Lacks Standing To Challenge the BOD.

To establish standing, a party must allege an injury to itself that is fairly traceable to the defendant's challenged conduct and likely to be redressed by the relief sought. "Causation, or 'traceability,' examines whether it is substantially probable that the challenged acts of the defendant, not of some absent third party, will cause the particularized injury of the plaintiff." *Fla. Audubon Soc'y v. Bentsen*, 94 F.3d 658, 663 (D.C. Cir. 1996). Redressability requires "that it be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." *Chamber of Commerce of the U.S. v. EPA*, 642 F.3d 192, 201 (D.C. Cir. 2011). Where, as here, "the requested relief consists solely of the reversal or discontinuation of the challenged action," "[t]he two requirements tend to merge." *Branton v. FCC*, 993 F.2d 906, 910 (D.C. Cir. 1993).

This case turns principally on the absence of these related elements. Kaspersky identifies its injuries as the loss of the right to sell to the government and the purported damage to the company's reputation and attendant commercial harm. Pls.' Mot. for Summ. J. at 17, ECF No. 19 (MSJ).

Kaspersky bears the burden to prove that these injuries are "likely" traceable to the challenged action and redressable by the requested relief. *Chamber of Commerce,* 642 F.3d at 201. As the government has explained, *see* Memo. in Opp'n to Pl.'s Application for a Prelim. Inj. at 14-22, ECF No. 13 (PI OPP), Kaspersky cannot carry that burden here. Where two laws independently produce the same alleged harm, a judicial decree overturning just one does not satisfy the redressability requirement. Here, rescinding the BOD would leave the congressional ban in place, which means federal agencies still would be required to remove and stop using Kaspersky products, and there still would be law branding the company's software as a security risk.

Challenging the NDAA ban in a separate lawsuit does not cure Kaspersky's redressability problem, and may very well concede it. Kaspersky has the burden of proving standing based on the facts as they existed at the time *this* suit was filed. Developments that occur after the complaint is filed are not relevant to the standing inquiry, and that is no less true for a post-filing lawsuit, even if it happens to be pending before the same judge and briefed on the same consolidated schedule. The company's new action neither changes the facts under consideration nor expands the potential relief available to Kaspersky in this case. If anything, it compounds the company's standing problems by conceding that the NDAA ban, standing alone, presents a live controversy.

A. Kaspersky's Loss of Its "Right to Sell to the Government" Is Not Redressable.

i. As the Government Has Shown, the NDAA Ban Forecloses Any Effective Relief from the Alleged Injury.

The government already has explained at length why rescinding the BOD will not redress Kaspersky's inability to sell software to the U.S. government. Rather than repeating the full analysis here, the government respectfully refers the Court to its opposition brief, which draws on a long line of standing cases to demonstrate why Kaspersky's decision to challenge only one of

multiple regulatory causes for its alleged injuries forecloses effective relief. *See* PI OPP at 14-22. The breadth and depth of the judicial consensus on this point is overwhelming: in circumstances where two laws independently produce the same alleged harm, the federal circuit courts unvaryingly conclude that a judicial decree overturning only one does not satisfy the redressability requirement for standing. *See, e.g.*, *Delta Const. Co. v. EPA*, 783 F.3d 1291, 1296 (D.C. Cir. 2015) (where two agencies issue "substantially identical" regulatory restrictions, vacating one agency's restrictions while leaving the other's in place would do nothing to redress the alleged harm), *reh'g denied en banc*, 2015 WL 5008257 (D.C. Cir. Aug. 3, 2015); *Physician's Educ. Network, Inc. v. Dep't of Health, Educ. & Welfare*, 653 F.2d 621, 623 (D.C. Cir. 1981) (where plaintiffs had based standing on the theory that rescinding a government report would forestall harmful legislation, the intervening passage of the legislation they had been hoping to forestall deprived them of a redressable injury); *see also* PI Opp at 16-19 (collecting cases).

This principle is not confined to cases where two laws proscribe the same conduct. Standing also fails where "governmental action is a substantial contributing factor in bringing about a specific harm, but the undoing of the governmental action will not undo the harm, because the new status quo is held in place by other forces." *Renal Physicians Ass'n v. U.S. Dep''t of Health & Human Servs.*, 489 F.3d 1267, 1278 (D.C. Cir. 2007). Especially relevant here are cases where the "other force" holding the new status quo in place is a statute, unchallenged in that case, which operates to ensure that third parties still will have incentive to continue their harmful conduct absent the challenged action. *See Nat'l Wrestling Coaches Ass'n v. Dept of Educ.*, 366 F.3d 930, 939 (D.C. Cir. 2004) (plaintiffs lacked standing to challenge agency's policy interpretation of a statute where it was the statute itself, and not the agency's gloss, that was causing third parties to take the allegedly harmful actions); *see also* PI OPP at 16-19 (collecting cases).

As the government has explained, these precedents compel the conclusion that the NDAA ban eliminates any possibility of judicial relief. Even though Section 1634(a) of the NDAA proscribes the same conduct as the BOD, the complaint in this suit challenges only the BOD. Rescinding the BOD would thus leave the full machinery of the congressional ban in effect, which means federal agencies would still be required to remove the company's software and the company would still be effectively excluded from federal business both before and after October 1.

It makes no difference, for purposes of standing, that the prohibition in the NDAA does not take effect until later this year. Even now, the ban "[holds] the new status quo . . . in place" by making the prospect of doing business with Kaspersky during the implementation period a practical (if not legal) impossibility. *See Renal Physicians Ass'n*, 489 F.3d at 1278. The NDAA ban embodies a legislative judgment that the security risk posed by Kaspersky software on federal networks is intolerably high. The broad scope of the ban shows that Congress contemplated a massive, government-wide implementation effort, and the timing of the ban—October 1 is a *deadline*, not a start date—together with the interim requirement for an inter-agency report on the authorities and procedures for removal of "suspect products," show that Congress assumed implementation efforts would begin immediately.

In these circumstances, where federal agencies are required to stop using Kaspersky products by October 1, both common sense and the realities of federal procurement dictate that lifting one prohibition just months before another takes effect would have no practical effect on the behavior of federal agencies. Although that principle should be self-evident, the government has submitted the declaration of Grant Schneider, the Federal Chief Information Security Officer (CISO), to reinforce the point. *See* Declaration of Grant Schneider ("Schneider Decl."), Dkt. 13-1. As Federal CISO and a former agency Chief Information Officer, Schneider is familiar with the rules and

principles governing federal IT procurement and regularly engages with executive branch CISOs and CIOs on information security matters. *Id*. ¶ 4. Based on this experience, he explains why he would find it inappropriate for any agency to purchase or install Kaspersky products before October 1, in light of the NDAA prohibition and the various factors—security, waste, procurement, fiscal, and technical—he explains in the Declaration. *Id*. at 6-7.

The bottom line is that Kaspersky's inability to sell products to the U.S. government is not dependent on the BOD and would exist whether or not the BOD is in effect. Agencies that recently removed the software to comply with the BOD would not repurchase it, and agencies that never had it would simply stay the course. Kaspersky would not recover lost licensing fees, and it would be no closer to a new sale than it was while the BOD was in force. The most Kaspersky could hope for is a narrow window, likely no more than several months, during which an agency could acquire and use Kaspersky software without breaking the law. But redressability turns on whether judicial intervention "will produce tangible, meaningful results in the real world," *Common Cause v. Dept. of Energy*, 702 F.2d 245, 254 (D.C. Cir. 1983), and must be "sufficient to take the suit out of the category of the hypothetical," *Sierra Club v. EPA*, 754 F.3d 995, 1001 (D.C. Cir. 2014). The abstract vindication Kaspersky would get from seeing the BOD overturned is not enough.

Kaspersky does not address the Schneider declaration, and it brushes aside the long line of D.C. Circuit decisions rejecting standing in cases where two laws independently produce the same alleged harm. *See, e.g.*, *Delta Constr. Co.*, 783 F.3d at 1296; *Physician's Educ. Network*, 653 F.2d at 623; *see also* PI OPP at 16-19 (collecting cases). Instead, Kaspersky falls back on the general principle that judicial relief can satisfy the redressability requirement if it constitutes "a necessary first step on a path that could ultimately lead to relief." MSJ at 22. The D.C. Circuit has confronted this argument in redressability cases involving injuries with multiple regulatory causes, and yet in

decision after decision, the court has found that a "first step" does not satisfy the redressability requirement where major legal impediments remain. *See, e.g., Delta Constr. Co.*, 783 F.3d at 1286 (removing one of two virtually identical regulatory restrictions does not satisfy redressability requirement); *Scenic Am., Inc. v. U.S. Dep't of Transp.*, 836 F. 3d 42, 53 (D.C. Cir. 2016) (where two government actions independently caused the alleged harm, "remov[ing] one of several barriers" to relief was not sufficient). Kaspersky has no response to these decisions, and the only case it counters with that is even remotely analogous is a thinly reasoned outlier from the District of Idaho. *See Idaho Bldg. & Const. Trades Council, AFL-CIO v. Wasden*, 32 F. Supp. 3d 1143 (D. Idaho 2014). That decision does not acknowledge, much less reconcile, the extensive body of case law denying standing in these circumstances, including Ninth Circuit precedent that directly contradicts its holding. *See, e.g.*, *Drakes Bay Oyster Co. v. Jewell*, 747 F.3d 1073 (9th Cir. 2014).

ii. Kaspersky Cannot Cure this Deficiency by Challenging the NDAA Ban in a Separate Lawsuit.

To the extent Kaspersky seeks to cure its redressability problem by challenging the NDAA ban in a separate lawsuit, its efforts are wasted. For one thing, the new lawsuit is not relevant to the standing inquiry in this case. "[S]tanding is to be determined as of the *commencement* of suit," *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 570-72 n.5 (1992) (emphasis added), and "may not be established by a development that occurs after the commencement of the litigation," *Park v. Forest Serv. of the U.S.*, 205 F.3d 1034, 1037-38 (8th Cir. 2000); *see Clapper v. Amnesty Int'l*, 568 U.S. 398, 426 (2013) ("We assess standing as of the time the suit is filed"). Further, standing is determined based on the relief available to the plaintiff in the case at bar. *See GAF Bldg. Materials Corp. v. Elk Corp. of Dallas*, 90 F.3d 479, 483 (Fed. Cir. 1996) (the proper focus in determining jurisdiction are "the facts existing at the time the complaint under consideration was filed").

This means the Court must assess standing based on the facts as they existed when the suit

commenced. If Kaspersky could not satisfy the redressability requirement on day one, then the case must be dismissed, regardless of any steps it later took (short of amending the complaint) to cure the deficiency. *Lujan*, 504 U.S. at 571-72 n.5. This rule is rigidly enforced, even where the post-filing development is a second lawsuit seeking relief which, had it been sought in the first suit, may have avoided the standing problem. *See Conservation Law Found. v. Pritzker*, 37 F. Supp. 3d 234, 243-44 (D.D.C. 2014). Although the two cases have been temporarily consolidated, the consolidation is "solely for the purpose of briefing an upcoming round of dispositive motions," Order (February 16, 2018), Dkt No. 17, which means the two actions will retain their separate status and procedural postures and will result in two separate judgments. *U.S. ex rel. Hampton v. Columbia/HCA Healthcare Corp.*, 318 F.3d 214, 216 (D.C. Cir. 2003) (unless two cases are consolidated "for all purposes," limited consolidation does not result in merger of the cases such that they would lose their separate identities). If Kaspersky wanted this Court to account for its challenge to the NDAA in assessing its standing to challenge the BOD, it could simply have amended the complaint. That at least would have expanded the remedial scope of the litigation and placed the two claims in the same procedural posture. By choosing to litigate the two claims separately, Kaspersky confined the standing analysis to the facts as they existed when this suit was filed, rendering the post-filing NDAA challenge irrelevant as a matter of law.

Even if the new lawsuit were relevant to the redressability question, the Court could not plausibly infer from the mere filing of a complaint that the NDAA ban is in jeopardy. While a court ordinarily can presume the plaintiff will prevail on the merits of its claim in assessing standing, no such presumption is afforded to claims in a separate lawsuit. *See US Ecology, Inc. v. U.S. Dep't of Interior*, 231 F.3d 20, 25-26 (D.C. Cir. 2000) ("The mere fact that appellant has brought [a separate suit about issues relevant to the redressability analysis] says nothing about the

underlying merits of those claims nor the remedy to which [appellant] would be entitled should it prevail."). Without that presumption, the Court could only speculate as to whether Kaspersky's new suit supports a likelihood that the NDAA ban will be struck down, such that rescinding the BOD could actually stand a chance of redressing Kaspersky's asserted injury. And even assuming such speculation were appropriate, as the government has explained, Kaspersky's bill of attainder claim is transparently flawed, and the prospect of finding that Kaspersky is entitled to relief in that case is virtually non-existent.

B. As the Government has Shown, Kaspersky's Reputational Injury Is Neither Redressable by a Favorable Decision Nor Fairly Traceable to the BOD.

The second component of Kaspersky's purported injury—the asserted damage to the company's reputation and attendant commercial harm—fails on both redressability and causation grounds. As the government has explained, the Court could not redress the reputational component of the injury (even assuming it could be fairly traced to the BOD), because there still would be a law on the books branding the company's software an information-security risk. If anything, Kaspersky's injury is *worse* under the NDAA, because the statutory ban exceeds the BOD in both the breadth of coverage (all federal information systems as opposed to the BOD's exclusion of national security systems and other systems used by DOD and the Intelligence Community) and the depth of its prohibition (all Kaspersky hardware, software, and services, including Kaspersky code embedded in third-party products, as opposed to the BOD's exclusion of embedded code and two specific Kaspersky services), while putting the force of Congress's legislative power behind a determination that the company's products are not safe for federal networks. No relief sought in this case can negate that judgment, and Kaspersky has not tried to explain, much less carried its burden of showing, how invalidating one stigmatizing government action only to leave a functionally identical one in place would provide meaningful relief. *See Paracha v. Obama*, 194

F. Supp. 3d 7, 10 (D.D.C. 2016) (Guantanamo detainee lacked standing to challenge federal statutes forbidding his relocation and labeling him a terrorist where he could not show that "the alleged harm to his reputation . . . is caused by the challenged statutes, rather than by the underlying facts of his detention or the Executive Branch's designation of petitioner as an enemy combatant," neither of which would be affected by a favorable ruling), *aff'd sub nom. Paracha v. Trump*, 697 F. App'x 703 (D.C. Cir. 2017).

Thus, in the same way that the NDAA ban forecloses the possibility of judicial relief from Kaspersky's inability to sell to the U.S. government, it ensures that overturning the BOD would not redress Kaspersky's asserted reputational harm by holding "the new status quo . . . in place." *Renal Physicians*, 489 F.3d at 1278. Indeed, the redressability problem is magnified in this context, because, as Kaspersky concedes in the NDAA suit, the congressional ban already has caused "profound reputational injuries," *see* NDAA Complaint ¶ 45, and because there are other forces, in addition to the NDAA ban, that are working to hold the new status quo in place. Those forces, discussed further below, include the removal of Kaspersky from GSA's contract schedules, and the countless statements, government actions, and press reports that have contributed to the company's notoriety. To the extent Kaspersky stands to gain anything from a favorable ruling, the "incremental" effect on its reputational interests would be too "vague and unsubstantiated" to support standing. *McBryde v. Comm. to Review Circuit Council Conduct & Disability Orders of Judicial Conference of U.S.*, 264 F.3d 52, 57 (D.C. Cir. 2001); *see Lebron v. Rumsfeld*, 670 F.3d 540, 562 (4th Cir. 2012) ("It is hard to imagine what 'incremental' harm it does to Padilla's reputation to add the label of 'enemy combatant' to the fact of his convictions and the conduct that led to them").

To make matters worse, Kaspersky's theory of redressability presupposes that this Court has authority to pass judgment on the sensitive, inherently discretionary judgments underlying the decision to issue the BOD. But as explained below, the decision to issue a BOD is committed to the Secretary's discretion and outside the scope of the APA. As a result, the *most* the Court could say about the merits of the BOD is that it was issued without adequate procedural protections, in violation of Kaspersky's right to due process. As the D.C. Circuit has recognized, it becomes impossible to show that a judicial declaration would redress a reputational injury when the court cannot pass judgment on the merits of the underlying findings. *See McBryde*, 264 F.3d at 57 (the court "could not see how" declaring Judicial Council acted *ultra vires* in suspending a judge would redress the judge's reputational injury when it would not affect the underlying findings).

But even supposing APA review were appropriate, for all the reasons discussed above, it would not be enough for the Court merely to declare that Kaspersky's software does not present a security threat to federal information systems. *See* Compl. at 22. If that were all the law required in reputational injury cases, "the redressability requirement [would] vanish," *Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 107 (1998), and a plaintiff could establish standing merely by pleading a causal link between reputational harm and governmental action, *Renal Physicians*, 489 F.3d at 1276. Rather, Kaspersky must show that it is likely, and not merely speculative, that the asserted harm to its reputation will be redressed by the requested relief. *Id*. That means explaining why, for instance, a customer who decided to remove Kaspersky products because, in the words of one Amazon reviewer, "the US gov't has banned the use of this software by all federal agencies," MSJ at 12, would be inclined to reconsider the decision if the BOD were overturned while the NDAA ban remained in place; or why the potential enterprise customers that withdrew from Kaspersky tenders purportedly "due to DHS's action" would be willing to reengage in a world where the

BOD were gone but the NDAA remained law, Angelo Gentile's Decl. in Supp. of Pls.' Motion for Summ. Judg. ¶ 19, ECF No. 10-2 ("Gentile Decl.").

Redressability aside, Kaspersky cannot show that its purported reputational harm is fairly traceable to the BOD, as opposed to the actions of third parties not before the Court. Where an "endless number of diverse factors potentially contribut[e]" to a particular injury, this "forecloses any reliable conclusion" that the injury is "fairly traceable" to the challenged action. *Winpisinger v. Watson*, 628 F.2d 133, 139 (D.C. Cir. 1980). That is the case here. By the time DHS issued the BOD, Kaspersky was already mired in controversy: six intelligence chiefs had publicly expressed concerns about the company's software, multiple congressional committees were investigating the company's connections to the Kremlin, GSA had started removal of Kaspersky from its schedules, a major national retailer had announced its decision to remove Kaspersky products from its stores, and Congress was poised to enact a government-wide ban. Kaspersky does not account for these actions in describing its reputational injuries, much less explain why the judgments they conveyed about the firm's products were any less harsh, or the blemishes they inflicted on the firm's reputation any less permanent, than those resulting from the BOD. As a result, the court has no way of determining whether the BOD plays a meaningful part in the causal story. *See Travis v. U.S. Dep't of Health & Human Servs,*. 2005 WL 589025, at *3 (D.D.C. Mar. 10, 2005) (denying standing where it was not clear whether the challenged action was a "deciding factor – or even a significant factor" in causing the harm).

Nor can Kaspersky identify a discernible nexus between the BOD and its declining revenues. Most of the firm's allegations on this score assume a causal relationship based on the temporal proximity of events, without considering, let alone controlling for other variables that are relevant to the analysis. For example, Kaspersky reports a 37 percent decline in third-quarter revenue,

attributing the loss to "[s]everal U.S. retailers" that removed Kaspersky products from their shelves "following the issuance of the BOD." Gentile Decl. ¶ 20. Nowhere does the company allege that it was the BOD, as opposed to the flurry of negative publicity or the various other government actions that preceded them, that prompted these retailers to suspend their partnerships. After all, Best Buy, the nation's largest consumer electronics retailer, cut ties with Kaspersky nearly a week *before* DHS issued the BOD. *See, supra*, note 14.

In short, Kaspersky has made it impossible for this Court to parse out the *legally relevant injury* – that is, the harm to the company's reputation and revenue stream resulting from the BOD, above and beyond the reputational harm resulting from other governmental, foreign, private, and media actions targeting the firm. *Katz v. Pershing, LLC*, 672 F.3d 64, 77 (1st Cir. 2012) (to satisfy Article III, "injury alleged . . . must be ascribable to the *defendant's* misrepresentations") (emphasis added). In these circumstances, where the challenged action is one among countless contributing factors, and where virtually all of the allegations supporting Kaspersky's theory of causation are not susceptible to being proven true or false, the Court has no reliable way of determining whether Kasperky's injuries are fairly traceable to the BOD.

Kaspersky's standing theory relies principally on the D.C. Circuit's decision in *Foretich v. United States*, where the plaintiff had standing to challenge a federal statute that restricted his right to visitation with his daughter—even though his daughter had already reached the age of majority—because there remained law on the books "embod[ying] a congressional determination that he engaged in criminal acts of child abuse from which his daughter needed protection." 351 F.3d 1198, 1211-13 (D.C. Cir. 2003). *Foretich*, however, does not carry the day for Kaspersky. If anything, the facts in that case bring Kaspersky's standing deficiencies into sharper relief.

The plaintiff's standing in *Foretich* rested on a straightforward causal relationship between the government action and the asserted reputational harm. *Id*. at 1214 ("Redress is possible in such a case because the damage to reputation is caused by the challenged action."). Traceability was easy to prove because there was no serious doubt that the asserted reputational injuries "resulted directly" from a single congressional action. *Id*. at 1211. Redressability was similarly straightforward because declaratory relief "would remove the imprimatur of government authority from an [a]ct that effectively denounces Dr. Foretich as a danger to his own daughter." *Id*. at 1215. The *Foretich* court did not have to untangle the consequences of multiple, overlapping government actions in determining whether the legally relevant injury could be fairly traced to the challenged statute. Nor did it have to assess redressability in light of an identical prohibition that would remain in place, along with the "imprimatur of government authority," after the challenged statute was gone. *Id*. Had the *Foretich* court faced those problems, it almost certainly would have reached a different outcome. At a minimum, it would have had to confront the long line of D.C. Circuit decisions denying standing in cases involving multiple, independent regulatory causes.[16]

II. Even if Kaspersky Has Standing, the United States Is Entitled to Summary Judgment on the Company's Due Process and APA Claims.

Summary judgment is warranted where "there is no genuine issue [of] material fact and . . . the moving party is entitled to a judgment as a matter of law." Fed. R. Civ. P. 56(c). Summary judgment is not only proper if a plaintiff fails to produce *any* evidence on an element of his case,

[16] Should the court determine that Kaspersky has standing to sue, it would still have sound prudential reasons to stay its hand. "In some circumstances, a controversy, not actually moot, is so attenuated that considerations of prudence and comity for coordinate branches of government counsel the court to stay its hand, and to withhold relief it has the power to grant.'" *City of New York v. Baker*, 878 F.2d 507, 509-10 (D.C. Cir. 1989) (citation omitted). Declining to hear a claim for equitable relief may be appropriate where, as here, "it is ... unlikely that the court's grant of declaratory judgment will actually relieve the injury." *Penthouse Int'l, Ltd. v. Meese,* 939 F.2d 1011 1019 (D.C. Cir. 1991).

but also if it fails to produce *sufficient* evidence on an element of his case. *Celotex Corp. v. Catrett*, 477 U.S. 317, 322 (1986).

A. The United States Is Entitled to Summary Judgment on Kaspersky's Due Process Claim.

Kaspersky has no reasonable basis for demanding administrative review prior to the issuance of the BOD. The BOD, it bears repeating, was *itself* "notice": it put Kaspersky on notice that DHS was requiring an action in 90 days, gathering information during that period, and reserving its right to change course based on new information presented during the review stage. That is the very definition of pre-deprivation process, but Kaspersky demands more. What Kaspersky actually wants is a pre-pre-deprivation process – that is, a complete process before the Department even announces an *initial* action.

The D.C. Circuit has established due process standards to apply in cases like this one, involving national security decisions that are based in part on classified information. The agency ordinarily must provide advance notice, furnish any releasable information on which the action is based, and allow an opportunity to present evidence to the decision-maker. *See, e.g.*, *People's Mojahedin Org. of Iran v. Dep't of State*, 327 F.3d 1238, 1242 (D.C. Cir. 2003).[17] The administrative process Kaspersky received was crafted with these standards in mind, and Kaspersky tacitly concedes that most of them have been satisfied. Kaspersky does not contend, for instance, that the content of the notice was deficient – *i.e.*, that the Secretary's memorandum should have been more detailed, or that the company was left guessing as to the basis for the agency's action. The company does not

[17] In circumstances where advance notice would impinge on U.S. national security goals, the agency may provide notice after the action is taken. *Holy Land Found. for Relief and Dev. v. Ashcroft*, 333 F.3d 156, 163 (D.C. Cir. 2003).

contend that it was denied an opportunity to oppose the Department's intended action, or that there was something unfair or unduly burdensome about the structure or operation of the review process.

Rather, Kaspersky's main grievance is that DHS should have notified the company sooner, before taking action that Kaspersky describes as an "immediate debarment" of Kaspersky from government business. MSJ at 1. The premise of this argument is Kaspersky's assertion that it was excluded from federal business "*upon the issuance* of the BOD." Compl. ¶ 9. As a result, any process that came after issuance of the BOD, the company asserts, is constitutionally deficient. Kaspersky says a "meaningful" process would have mirrored the pre-deprivation procedures used for the suspension and debarment of federal contractors. MSJ at 32. As explained below, debarment is not an appropriate model for evaluating this due process claim, and Kaspersky's analogy to debarment procedures overstates the process to which it was constitutionally entitled. Further, even if the debarment procedures were an appropriate benchmark, the process afforded to Kaspersky not only meets it, but even exceeds it in important ways.

i. Assuming It Was Entitled To It, Kaspersky Received Adequate Pre-Deprivation Process.

Kaspersky's pre-deprivation argument, indeed its entire due process claim, rests on a basic misconception about how the BOD works. Contrary to the company's assertion, the BOD did *not* require the immediate removal of Kaspersky products from federal information systems. Instead, it began a 90-day fact-finding process that would eventually culminate in removal, but *only if* agencies were not "directed otherwise by DHS in light of new information." AR 635. During this period, agencies reported to DHS with information about the Kaspersky products on their systems, and Kaspersky came forward with detailed written arguments opposing DHS's intended action. No directive to begin removing Kaspersky products took effect until the information-gathering stage was complete and the Acting Secretary reached a final decision based on all the evidence.

These procedures bear all the hallmarks of pre-deprivation process, and they certainly are no less timely or effective than the federal debarment process, which Kaspersky itself recognizes is constitutionally adequate. MSJ at 32. As with the debarment process, the BOD provided Kaspersky prompt notice of the action being considered, a thorough explanation of the unclassified reasons for considering it (including a 21-page memorandum with 47 exhibits), and an opportunity (52 days – more than three weeks longer than the 30 days required under the FAR, 48 C.F.R. § 9.406-3(c)) to contest disputed facts before the agency reached a final decision on the proposed action. And as with the debarment process, the BOD deferred a final decision until after the decision-maker had reviewed all relevant information, including information submitted by aggrieved parties. If anything, the debarment procedures afford *less* pre-deprivation process, because a "proposed debarment" results in a contractor's immediate exclusion from federal business pending a final decision from the debarment officer. *Id*. § 9.405. Issuing the BOD, by contrast, had no such preclusive effect: while federal agencies were required, upon issuance of the BOD, to identify Kaspersky products on their systems and develop plans for removal, it was clear from the outset that the requirement to implement those plans was subject to the outcome of DHS's review process.

Kaspersky condemns this administrative process as "illusory," insisting that the BOD, by setting in motion a process for identification and removal of the company's products, "prejudiced" federal agencies against Kaspersky, such that "the process could therefore not have been adequately unwound." Compl. ¶ 9. This argument mistakes voluntary risk-management decisions with legal compulsion. The agencies that removed Kaspersky software before the 90-day mark did so on their own initiative, without any direction from DHS. Those independent risk-management decisions, which could have resulted from a combination of any of the executive and legislative actions described above, did not amount to a constitutional deprivation and therefore did not trigger

due process protections. *See, e.g.*, *Legal Tender Cases*, 79 U.S. 457, 551, 20 L. Ed. 287 (1870) (due process refers to "a direct appropriation, and not to consequential injuries resulting from the exercise of lawful power"). The "complete debarment" Kaspersky repeatedly refers to was not enacted by the provisional order; the requirement to remove and discontinue use came only after the Acting Secretary made the final decision to maintain the removal requirement without modification. Because *that* action forms the basis for Kaspersky's alleged constitutional injury, *see* Compl. ¶ 34, it is the process surrounding that action that governs Kaspersky's due process claim.[18] *See O'Bannon v. Town Court Nursing Ctr.*, 447 U.S. 773, 789 (1980) (due process is not concerned with "consequential injuries resulting from the exercise of lawful power").

ii. Kaspersky Was Not Entitled to Notice Prior to The Department's Provisional Action.

As set forth above, the pre-deprivation process Kaspersky received was comparable to, and in some respects greater than, what Kaspersky calls the "well-established" and "constitutionally adequate" debarment procedures, and any differences between the two procedures are not of constitutional dimension. That should end the matter, but even if the court were to conclude that the BOD's review process somehow falls short of the federal debarment procedure, it would not follow that the review process violates due process.

Under the familiar test of *Mathews v. Eldridge*, whether process is constitutionally adequate depends on balancing three factors: (1) "the private interest that will be affected by the official action"; (2) "the risk of an erroneous deprivation of such interest through the procedures used, and the probable value, if any, of additional or substitute procedural safeguards"; and (3) "the

[18] To hold otherwise would be to render any provisional order final depending on the potential actions of third parties, whether predictable or entirely unknowable. An agency may choose to change their procedures in response to a proposed rule or action by another, but that does not render the initial action final and binding on third parties until it has been issued in final form.

Government's interest, including the . . . fiscal and administrative burdens that the additional or substitute procedural requirement would entail." 424 U.S. 319, 335 (1976). How to satisfy due process's meaningful-opportunity requirement is informed by context, and, accordingly, due process procedures may vary "'depending upon the importance of the interests involved."' *Cleveland Bd. of Educ. v. Loudermill*, 470 U.S. 532, 545 (1985).

Due process is always context-specific, requiring that private injury be weighed against the government's interest and the probable value of additional procedural protections. *Mathews*, 424 U.S. at 335; *see also Morrissey v. Brewer*, 408 U.S. 471, 481 (1972) ("due process is flexible and calls for such procedural protections as the particular situation demands."). When properly balanced, the government's interest in responding quickly and nimbly to imminent, potentially catastrophic cyber threats is entitled to significant weight, and the process Kaspersky received was more than sufficient to satisfy the Constitution. *See Cafeteria & Rest. Workers Union v. McElroy*, 367 U.S. 886, 896 (1961) (no hearing was required where Navy revoked employee's security clearance because the governmental function at issue was "to manage the internal operation of an important federal military establishment").

First, the United States has a compelling interest in maintaining the flexibility to take effective action in response to cybersecurity risks. *Haig v. Agee*, 453 U.S. 280, 307 (1981) ("no governmental interest is more compelling than the security of the Nation"). Our Constitution recognizes that sensitive decisions about national security belong in the hands of those who are best positioned to make them. *Dep't of Navy v. Egan*, 484 U.S. 518, 530 (1988). Congress made the same judgment when it granted the Secretary broad authority to take protective measures in this area, and the absence of any requirement in the BOD authority for the procedural participation of private parties adversely affected by a BOD is a testament to Congress's desire for swift,

unencumbered action. The government's cybersecurity interests should weigh heavily in the balance, more so than the government's interests in the debarment context, where a significant concern is curbing fraud and waste. *See Caiola v. Carroll*, 851 F.2d 395, 399 (D.C. Cir. 1988) ("Debarment reduces the risk of harm to the system by eliminating . . . the unethical or incomplete contractor"). Indeed, in cases where an alleged debarment implicates national security concerns, the procedural protections ordinarily afforded to contractors may be significantly diminished. *See MG Altus Apache Co. v. United States*, 111 Fed. Cl. 425 (Ct. Fed. Cl. 2013).

Further, Kaspersky's private interests were well protected by the government's publicized procedures, and the risk of erroneous deprivation and the probable value of different safeguards is slight. "The function of legal process, as that concept is embodied in the Constitution, and in the realm of fact-finding, is to minimize the risk of erroneous decisions." *Greenholtz v. Inmates of Neb. Penal and Correctional Complex*, 442 U.S. 1, 13 (1979). The private interest considered at this stage is that of "the *erroneously* [deprived] individual." *Hamdi v. Rumsfeld*, 542 U.S. 507, 530 (2004); *Carey v. Piphus*, 435 U.S. 247, 259 (1978) ("Procedural due process rules are meant to protect persons not from the deprivation, but from the mistaken or unjustified deprivation…."). The BOD reduced the risk of error by ensuring that the government accounted for all relevant information and that aggrieved parties had an opportunity to draw the government's attention to any possible errors. Kaspersky had an opportunity to engage DHS, to oppose the action, and to propose any mitigating measures before the agency made a final decision affecting the company's legal rights. DHS then closely examined all aspects of Kaspersky's submission, as evidenced by the detailed, 25-page December 4 memorandum to the Acting Secretary. AR 752-776. There is no reason to believe that providing this process earlier would have yielded a different result.

The suggestion that earlier process could reduce the risk of "error" is all the more implausible in light of the purpose of FISMA, which is to safeguard against the *risk of* cyber intrusions – not, as Kaspersky suggests, to *conclusively prove* them. FISMA is not a criminal statute and the BOD authority does not require proof that someone has committed a security breach or violated a security standard; rather, it is a risk-avoidance authority that requires only a "known or reasonably suspected" threat, vulnerability, or risk. 44 U.S.C. § 3552(b)(1). Some of the risks the Secretary identifies in carrying out her authority may never mature or take shape. But that does not mean it was error for the Secretary to address those risks in the first place.

Just as Kaspersky overstates the value of earlier process, it unduly plays down the government's sensitive and weighty interests in acting promptly. Kaspersky makes the puzzling assertion that the record is devoid of any reasons for "urgency and immediacy," MSJ at 36, as if the prospect of a foreign adversary gaining access to U.S. federal networks were not reason enough for swift action. The evidence shows that nation states with highly sophisticated cyber programs are targeting U.S. networks on a "daily basis," A.R. 106; that the threat from Russia is particularly "severe" and unlikely to abate, A.R. 65; and that, in addition to the potential consequences for U.S. public health and safety, a successful cyber intrusion could give adversaries like Russia "new avenues for coercion and deterrence," A.R. 66. These threats demand immediate attention, and DHS has an interest in avoiding any administrative process that would further divert the focus of cybersecurity officials engaged in the serious work of protecting federal networks, particularly where such process would have to precede even a *provisional* action.

In short, Kaspersky's demand for earlier notice is unwarranted in light of its limited "probable value" and the burdens it would impose on the government in the cybersecurity area. *Mathews*, 424 U.S. at 335. The process Kaspersky received was more than enough to satisfy the

constitutional standard. DHS gave Kaspersky notice of its intended action and an opportunity to introduce information in response. In the meantime, agencies were able to take certain preliminary steps that would allow them to act swiftly at day 90 if not directed otherwise. This process strikes an appropriate balance between Kaspersky's interest in receiving information about the decision and having an opportunity to respond, and the Department's interest in acting promptly and effectively in response to emerging cyber threats.

B. Kaspersky Was Not Entitled to Respond to the Maggs Report.

Finally, Kaspersky contends that DHS deprived it of due process by submitting the Maggs Report at the final stage of the administrative process (rather than introducing it with the BOD), thereby denying Kaspersky an opportunity to address it. MSJ at 37-38. Kaspersky offers no authority for the assertion that the Fifth Amendment is implicated by a supplemental report that builds on information provided at an earlier stage of the administrative process. The due process question, rather, is whether Kaspersky was given access to the unclassified grounds for the agency's action and an opportunity to rebut them. *See Ralls Corp. v. Comm. on Foreign Inv. in the U.S.*, 758 F.3d 296 (D.C. Cir. 2014).

That is precisely what happened here. The initial memorandum detailed the Department's concern that Russian law could be used to facilitate the FSB's exploitation of Kaspersky software. AR 14-16. It cited specific, key Russian laws, including provisions of concern, and discussed, among other authorities and levers of political influence, the FSB's authority to compel assistance from Russian companies; its authority to second FSB personnel to Russian companies with the head of the enterprise's consent; its authority to request that electronic communications service providers install interception hardware and software; and its ability to intercept data transmissions made over Russian telecom and internet service provider networks. *Id*. The findings and

conclusions provided in the Maggs Report expanded upon these issues, adding nuance and tying them to additional provisions of Russian law. In these circumstances, Kaspersky is incorrect that it was unable to meaningfully respond to DHS's concerns about Russian law.

Further, Kaspersky's suggestion that it was entitled to review and respond to all of the unclassified information the Acting Secretary was considering (rather than the 21-page memorandum it received at the beginning of the administrative process) is inconsistent with how agencies make decisions in this context. Being required to provide all information at the beginning of the administrative review could paralyze an agency by leaving it perpetually vulnerable to the charge that a late-received piece of information should have been disclosed to the applicant sooner, or, if disclosed, result in yet another round of administrative correspondence. This reasoning, if adopted, would subject agencies to a never-ending cycle of administrative correspondence, hampering their ability to exercise statutory authority and threatening their core missions.

III. The United States Is Entitled to Summary Judgment on Kaspersky's APA Claim.

Kaspersky's APA claim fails at the threshold. The APA precludes judicial review where "agency action is committed to agency discretion by law," 5 U.S.C. § 701(a)(2), as FISMA does by giving the DHS Secretary unreviewable discretion to identify and eliminate threats. But even if APA review were appropriate, the decision to issue the BOD would easily withstand it: there is substantial evidence to support the Acting Secretary's finding that Kaspersky software presents a known or reasonably suspected threat, vulnerability, or risk to federal information and information systems, and the rational connection between that finding and the removal order is plain. Particularly in light of the heightened deference that is due to agency decisions in the sensitive area of national security, as well as the deference built into FISMA itself, the government is entitled to summary judgment on the merits of Kaspersky's APA claim.

The Acting Secretary's decision to issue the BOD is not subject to APA review. The APA provides for judicial review of all "final agency action for which there is no other adequate remedy in a court," 5 U.S.C. § 704, except when "statutes preclude judicial review" or the "agency action is committed to agency discretion by law." *Id.* § 701(a). APA review is precluded under 5 U.S.C. § 701(a)(2) when a "statute is drawn so that a court would have no meaningful standard against which to judge the agency's exercise of discretion." *Heckler v. Chaney*, 470 U.S. 821, 830 (1985). In other words, "'there is no law to apply."' *Citizens to Preserve Overton Park, Inc. v. Volpe*, 401 U.S. 402, 410 (1971). In making this assessment, the D.C. Circuit considers three principal factors: (i) "the language and structure of the statute that supplies the applicable legal standards for reviewing that action," (ii) "Congress's intent to commit the matter fully to agency discretion as evidenced by . . . the statutory scheme," and (iii) "the nature of the administrative action at issue." *Watervale Marine Co. v. U.S. Dep't of Homeland Sec.*, 55 F. Supp. 3d 124, 137-38 (D.D.C. 2014) (citations omitted), *aff'd on other grounds sub nom.*, 807 F.3d 325 (D.C. Cir. 2015). Applied here, all three factors compel the conclusion that APA review is foreclosed.

First, FISMA provides insufficient standards for the Court to apply. The BOD was issued under the Secretary's authority under FISMA to issue binding operational directives to "safeguard[] Federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk." 44 U.S.C. §§ 3552(b)(1), 3553(b)(2). There is no legal test for what constitutes "a known or reasonably suspected information security threat, vulnerability, or risk," and no legal standard for determining whether a particular directive to "safeguard" goes too far or not far enough. *Id*. Congress did not provide any guidance on what factors or criteria the Secretary should consider in exercising her authority. Instead, it vested complete discretion in the Secretary to make judgments about cyber threats that may warrant invocation of the BOD

authority. Indeed, FISMA provides the Secretary with discretion not only to issue a BOD, but also to use a variety of other measures to enforce compliance with cybersecurity policies. The "breadth of the authorized tools that the [Secretary] can bring to bear on the problem, and the fact that the agency has discretion to use any and all of them," shows Congress's deference to the Secretary and its recognition of her expertise in this area. *Watervale Marine Co.*, 55 F. Supp. 3d at 143-44.

Second, Congress's deferential approach "permeates the 'overall structure' of the statute," *id.* at 139, lending further support to the conclusion that the decisions agencies make in connection with their FISMA obligations are not subject to APA review. FISMA divides and assigns broad discretionary authorities between the Director of OMB, the Secretary of DHS, and individual agencies. Among other authorities, the OMB Director is authorized to "develop[] and oversee[] the implementation of policies, principles, standards, and guidelines on information security," 44 U.S.C. § 3553(a)(2), and the Secretary of DHS is broadly authorized to "administer the implementation of agency information security policies and practices for information systems," including assisting the Director in carrying out OMB authorities, convening meetings with senior agency officials to help ensure effective implementation of information security policies and practices, and developing and implementing BODs. *Id.* § 3553(b). Finally, agencies have broad discretion and responsibility for providing information security protections "commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction" of agency information and information systems. *Id.* § 3554(a)(1)(A).

Indeed, the courts that have considered the issue have unanimously concluded that the choices an agency makes in carrying out its obligations under FISMA are not susceptible to APA review. FISMA, they have recognized, "is a peculiarly hortatory statute directed to federal executives to protect federal information technology for the benefit of the federal government." *Welborn v. IRS*,

218 F. Supp. 3d 64, 81 (D.D.C. 2016). The deferential approach is reflected in the statutory scheme, in which "[t]here is no private right of action" and "each agency head is delegated full discretion in determining how to achieve its goals, which removes it from APA review." *Id.*; *see also In re U.S. Office of Pers. Mgmt. Data Sec. Breach Litig.* ("*OPM Litigation*"), 266 F. Supp. 3d 1, 44 (D.D.C. 2017) ("The Court holds that OPM's actions in carrying out the statute's requirements is committed to the agency's discretion, and not subject to judicial review under the APA."). And the D.C. Circuit has recognized the absence in the statute of any "role for the judicial branch," noting that it is "far from certain that courts would ever be able to review the choices an agency makes in carrying out its FISMA obligations." *Cobell v. Kempthorne*, 455 F.3d 301, 314 (D.C. Cir. 2006).[19] *OPM Litigation*, *Welborn*, and *Cobell* each affirm the complete discretion granted to agencies to decide how to secure their information systems, and the Secretary's authority to issue BODs is at least as broad and discretionary as the authorities these courts found to be committed to agency discretion.

The final consideration—the nature of the administrative action—refers to "certain categories of administrative decisions" that the Supreme Court and the D.C. Circuit consider presumptively unreviewable. *Sec'y of Labor v. Twentymile Coal Co.*, 456 F.3d 151, 156 & n. 6 (D.C. Cir. 2006) (collecting cases). The initial determination as to whether the known facts and intelligence about a particular cybersecurity threat warrant government-wide action involves the review and analysis of sensitive, often classified intelligence, coupled with the understanding and analysis of an ever-evolving cybersecurity environment. Further, the information and analysis underlying these

[19] *Cobell*, decided in 2006, relates to FISMA 2002, enacted as Title III of the E-Government Act of 2002. Pub. L. No. 107-347, 116 Stat. 2899 (2002). Still, the decision applies with equal force to the current FISMA, which, like FISMA 2002, provides no role for the judicial branch.

decisions tends to be expert-driven and highly technical, and this case was no exception. *See, e.g.*, AR 25-32 (information security risk assessment prepared by NCCIC).

Courts must give "an extreme degree of deference to the agency when it is evaluating scientific data within its technical expertise," *Huls Am., Inc. v. Browner*, 83 F.3d 445, 452 (D.C. Cir. 1996) (citations omitted). That is especially true here, where the government must "confront evolving threats in an area where information can be difficult to obtain and the impact of certain conduct difficult to assess," and where the "the lack of competence on the part of the courts is marked, [] and respect for the Government's conclusions is appropriate." *Holder v. Humanitarian Law Project*, 561 U.S. 1, 34 (2010). The threat assessments underlying DHS's BOD authority are not unlike the decision to grant or deny an individual's security clearance – a decision which the courts have recognized is entirely discretionary. *See Egan*, 484 U.S. at 529. The judicial admonition that "[c]ourts are in no position to gauge what constitutes an acceptable margin of error for determinations that bear on national security," *Oryszak v. Sullivan*, 565 F. Supp. 2d 14, 19-20 (D.D.C. 2008), applies equally here.

Kaspersky does not meaningfully engage the framework for determining whether an action is committed to an agency's discretion. Instead, the company rests its case for APA review on the *consequences* of the BOD, insisting that judicial review is necessary because the BOD "effectuated a debarment." MSJ at 40. Kaspersky's focus on consequences ignores controlling precedent and turns the reviewability analysis on its head. The question is whether there is a "meaningful standard against which to judge the agency's exercise of discretion," *Heckler*, 470 U.S. at 830, not whether the adverse effects of the challenged action resemble those of other agency actions subject to APA review. While such adverse effects may entitle a company to certain procedural protections,

Gonzalez v. Freeman, 334 F.2d 570, 578 (D.C. Cir. 1968), they do not expand the judicially settled scope of the APA or render an otherwise unreviewable action reviewable.

Even if the decision were not committed to agency discretion, the APA claim still fails on the merits. Under the APA, a court reviews an agency decision based on the administrative record. *Fla. Power & Light Co. v. Lorion*, 470 U.S. 729, 743-44 (1985). An agency decision should be upheld unless it is (as relevant here) "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. § 706(2). The Court's review under this standard is narrow and highly deferential, and the Court does not substitute its judgment for that of the agency. *See Citizens to Preserve Overton Park*, 401 U.S. at 416. The agency's decision should be affirmed as long as it is supported by a rational basis. *Jifry v. FAA*, 370 F.3d 1174, 1181 (D.C. Cir. 2004) ("The court must affirm the agency's findings of fact if they are supported by substantial evidence' and there is a rational connection between the facts found and the choice made." (citation omitted)).

Because DHS's action implicates national security, it is due even greater deference than ordinarily applies under the APA. *See Regan v. Wald*, 468 U.S. 222, 242 (1984) ("Matters relating 'to the conduct of foreign relations . . . are so exclusively entrusted to the political branches of government as to be largely immune from judicial inquiry or inference"' (citation omitted)). The Supreme Court has emphasized the need for courts to afford this heightened deference, even when considering constitutional claims, because courts should respect the executive branch's expertise in the national security and foreign policy arena. *Humanitarian Law Project*, 561 U.S. at 33-34; *see also Islamic Am. Relief Agency v. Gonzales ("IARA")*, 477 F.3d 728, 734 (D.C. Cir. 2007) ("[W]e reiterate that our review—in an area at the intersection of national security, foreign policy, and administrative law—is extremely deferential"). APA and national security deference are even more crucial when considered in conjunction with the broad discretion found in FISMA itself,

which vests the Secretary with sweeping authority to take such actions as she deems necessary to secure federal information systems against cyber threats.

Notwithstanding the deference owed to agency decisions that, like this one, directly implicate national security, Kaspersky claims that the BOD is arbitrary and capricious because DHS: (1) relied on media reports in building the evidentiary record; (2) failed to present "conclusive evidence that Kaspersky Lab had facilitated any breach" of U.S. national security; and (3) failed to show that Kaspersky software poses a greater "technical risk" to federal information systems than similar software used by the government. MSJ at 41-44. None of these arguments has merit.

First, there is no merit to Kaspersky's contention that DHS improperly relied on news reports, purportedly at the expense of "meaningful agency fact-finding." MSJ at 1. To the extent Kaspersky contends there was something procedurally improper about relying on news reports, its argument is foreclosed by D.C. Circuit precedent, which repeatedly has "approved the use of such materials as part of the unclassified record" in national security cases. *Zevallos v. Obama*, 793 F.3d 106, 113 (D.C. Cir. 2015); *see, e.g.*, *People's Mojahedin Org. of Iran v. U.S. Dep't of State*, 182 F.3d 17, 19 (D.C. Cir. 1999) ("nothing in [AEDPA] restricts [the Department of State] from acting on the basis of third hand accounts, press stories, material on the Internet[,] or other hearsay regarding the organization's activities"); *Holy Land*, 333 F.3d at 162 ("[I]t is clear that the government may decide to designate an entity based on a broad range of evidence, including intelligence data and hearsay declarations"). As these decisions recognize, "[t]here are good reasons" to permit agencies to rely on these materials in national security matters, particularly where the challenged action is "based in part on classified information." *Zevallos*, 793 F.3d at 113 (explaining that various legal, diplomatic, and logistical obstacles "may limit what [an agency] or its agents can say publicly").

Further, it is simply not accurate to say that news reports constituted the "principal and overwhelming" source of evidence provided in support of the BOD. MSJ at 3. DHS's decision is supported by a robust administrative record, including two evidentiary memoranda prepared by the Assistant Secretary for Cybersecurity and Communications, who herself relied on research and analysis from cybersecurity experts in the Department's National Protection and Programs Directorate, including two risk assessments prepared by the NCCIC, and a report on relevant aspects of Russian law. Those memoranda and assessments relied on a wide range of sources other than news reports. Where DHS relies on news reports, it is invariably in connection with facts that Kaspersky could readily rebut or disprove, and it is telling that Kaspersky's summary judgment brief does not identify a single report that is inaccurate or unreliable.

Second, Kaspersky repeatedly states that DHS has presented no evidence of any "breach" or "wrongdoing" connected with its software. MSJ at 30, 44. This argument misses the central purpose of the BOD. To secure the U.S. government's information systems, the Secretary must be able to take protective measures based on sensitive, predictive judgments about the threats facing U.S. networks. This authority is by nature forward-looking; it covers both "known" and "*reasonably suspected*" threats, vulnerabilities, and risks, and is in no way limited to prior breaches or actors that have carried out malicious activity in the past. As long as Kaspersky products were present on federal information systems, Russia would have the ability to exploit Kaspersky's access to those information systems, with potentially grave consequences to U.S. national security. That is a risk DHS is unwilling to accept – and one well within its authority to address.

Finally, Kaspersky contends that DHS failed to demonstrate the "technical risk" posed by Kaspersky software relative to other antivirus software used by federal agencies. Kaspersky also faults DHS for focusing on security risks associated with antivirus software generally, rather than

independent testing and evaluation of Kaspersky products. And it contends that a report from the Berkeley Research Group (BRG), a consulting firm Kaspersky retained in connection with this litigation, shows that Kaspersky products pose no greater risk to federal information systems than antivirus software provided by other vendors. MSJ at 43-44.

These arguments conflate two distinct aspects of the DHS's justification for the BOD: concerns about the way Kaspersky antivirus software operates, and concerns about Russian agents finding ways to use Kaspersky software on federal networks as a platform to conduct cyber operations. With respect to the operation of Kaspersky software, DHS's concerns stem primarily from what the company's software has in common with modern antivirus software. AR 758-59. The determination that Kaspersky-branded products present an information security risk was not based on the unique technical features of Kaspersky products, but rather the broad access and privileges antivirus software is afforded by design. AR 759. Kaspersky does not dispute this aspect of DHS's findings, and the BRG report actually confirms some of DHS's key conclusions. AR 759.

With respect to the threat of Russian exploitation, the exceptional risk Kaspersky poses relative to other antivirus providers is not seriously controverted. DHS considered BRG's assessment that other software providers pose comparable risks and responded at length during the administrative review process. As relevant here, DHS concluded that "none of the antivirus developers or their products present the same information security risks that DHS has identified with respect to Kaspersky-branded products." AR 770. While some of the vendors identified by BRG have isolated features in common with Kaspersky, none presents anything close to the threat profile DHS has documented in the administrative record. For example, BRG identifies three vendors with "offices" in Russia, but it never describes the scope or nature of those offices, nor does it suggest that any of these vendors have headquarters or back-end servers there, let alone unusually

close ties to the Russian intelligence services. AR 771. Likewise, while other software vendors have networks that enable them to collect user data and transfer it to third parties in other countries, such networks would not present a comparable security risk absent evidence that Russian actors could use them to access data for malicious purposes. AR 772.

At the end of the day, the APA challenge amounts to a disagreement with DHS's determination that the presence of Kaspersky's antivirus software on federal information systems rises to the level of a security risk. But an agency's determination and explanation are not arbitrary or capricious simply because the plaintiff, or even the court, disagrees with its conclusion. The Supreme Court has emphasized that "[m]atters intimately related to foreign policy and national security are rarely proper subjects for judicial intervention." *Haig*, 453 U.S. at 292. This case is not the rare exception. Congress entrusted the security of the federal government's information systems to the Secretary, and this Court should decline Kaspersky's invitation to second-guess her determination that Kasperky's software poses an unacceptable risk to the nation's security.

CONCLUSION

The Court should dismiss this suit for lack of jurisdiction or, alternatively, deny Kaspersky's motion for summary judgment and grant the government's cross-motion.

Dated: March 26, 2018

Respectfully submitted,

CHAD A. READLER
Acting Assistant Attorney General
ERIC R. WOMACK
DIANE KELLEHER
Assistant Branch Directors
Civil Division
/s/ Samuel M. Singer
SAMUEL M SINGER (D.C. Bar 1014022)
Trial Attorney, United States Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave, NW; Washington, D.C. 20530;
(202) 616-8014; samuel.m.singer@usdoj.gov