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' APPLICATION FOR A PRELIMINARY INJUNCTION

TABLE OF CONTENTS

INTRODUCTION 1

BACKGROUND 4

I. Statutory Background 4

II. Factual Background 5

a. Kaspersky's Software and Connections to Russia 5

b. Kaspersky Comes under Public Scrutiny 7

c. The Binding Operational Directive 10

d. The National Defense Authorization Act of 2018 13

DISCUSSION 14

I. Kaspersky Lacks Standing To Challenge the BOD 14

a. Kaspersky's Loss of Its "Status as a Vendor" Is Not Redressable Because the NDAA Ban Forecloses Any Effective Judicial Relief from the Alleged Injury. 15

i. Any Harm Stemming from Kaspersky's Inability to Sell to the United States Is Not Redressable 19

ii. Kaspersky's Reputational Is Neither Redressable by a Favorable Decision Nor Fairly Traceable to the BOD. 22

II. Kaspersky Is Not Entitled to a Preliminary Injunction 27

a. Kaspersky Is Unlikely To Prevail on the Merits 28

i. Kaspersky Has Failed to State a Procedural Due Process Claim 28

1. Assuming It Was Entitled To It, Kaspersky Received Adequate Pre-Deprivation Process. 29

2. Kaspersky Was Not Entitled to Notice Prior to The Department's Proposed Action. 31

3. Kaspersky Was Not Constitutionally Entitled to Respond to the Maggs Report. 34

ii. Kaspersky Has Failed to State a Claim under the Administrative Procedures Act 35

III. Kaspersky Will Not Suffer Irreparable Harm Absent a Preliminary Injunction 42

IV. The Balance of Equities Favor the Government..... 43

CONCLUSION..... 45

TABLE OF AUTHORITIES

CASES

Abdullah v. Obama,
753 F.3d 193 (D.C. Cir. 2014) 28

Adams v. Vance,
570 F.2d 950 (D.C. Cir. 1978) 44

Advantage Media, LLC v. City of Eden Prairie,
456 F.3d 793 (8th Cir.2006) 16

Boddie v. Connecticut,
401 U.S. 371 (1971) 32

Branton v. FCC,
993 F.2d 906 (D.C. Cir. 1993) 14

Caiola v. Carroll,
851 F.2d 395 (D.C. Cir. 1988) 33

Chamber of Commerce v. EPA,
642 F.3d 192 (D.C. Cir. 2011) 14, 15

Citizens to Preserve Overton Park, Inc. v. Volpe,
401 U.S. 402 (1971) 36, 39

City of New York v. Baker,
878 F.2d 507 (D.C. Cir. 1989) 27

Cleveland Bd. of Educ. v. Loudermill,
470 U.S. 532 (1985) 32

Cobell v. Kempthorne,
455 F.3d 301 (D.C. Cir. 2006) 38

Common Cause v. Dept. of Energy,
702 F.2d 245 (D.C. Cir. 1983) 22

Delta Const. Co. v. EPA,
783 F.3d 1291 (D.C. Cir. 2015) 16

Akinseye v. D.C.,
339 F.3d 970 (D.C. Cir. 2003) 14

Drakes Bay Oyster Co. v. Jewell,
747 F.3d 1073 (9th Cir. 2014) 16

Dynatlantic Corp. v. Dep't of, Def, 115 F.3d 1012 (D.C. Cir. 1997) 15

Fla. Audubon Soc'y v. Bentson, 94 F.3d 658 (D.C. Cir. 1996) 14

Fla. Power & Light Co. v. Lorion, 470 U.S. 729 (1985) 39

Global Relief Found. v. O'Neill, 207 F. Supp. 2d 779 (N.D. Ill. 2002), *aff'd*, 315 F.3d 748 (7th Cir. 2002) 44

Greenholtz v. Inmates of Neb. Penal and Correctional Complex, 442 U.S. 1 (1979) 33

Gulf Oil Corp. v. Fed. Energy Admin., 391 F. Supp. 856 (W.D. Pa. 1975) 44

Haig v. Agee, 453 U.S. 280 (1981) 33, 44

Harisiades v. Shaughnessy, 342 U.S. 580 (1952) 44

Heckler v. Chaney, 470 U.S. 821 (1985) 36

Hodges v. Abraham, 253 F. Supp. 2d 846 (D.S.C. 2002) 44

Holder v. Humanitarian Law Project, 561 U.S. 1 (2010) 38, 40

Holy Land Found. for Relief and Dev. v. Ashcroft, 333 F.3d 156 (D.C. Cir. 2003) 29, 41

Huls America, Inc. v. Browner, 83 F.3d 445 (D.C. Cir. 1996) 38, 40

Huntington Branch, N.A.A.C.P. v. Town of Huntington, 689 F.2d 391 (2d Cir. 1982) 22

In re U.S. Office of Pers. Mgmt. Data Sec. Breach Litig., 266 F. Supp. 3d 1 (D.D.C. 2017), *appeals filed*, Nos. 17-5217 (D.C. Cir. 2017), 17-5232 (D.C. Cir. 2017), *sub. nom, AFGE, AFL-CIO v. OPM*, No. 18-1182 (Fed. Cir. 2017) 37

Int'l Union of Bricklayers & Allied Craftsmen v. Meese, 761 F.2d 798 (D.C. Cir.1985) 22

Islamic Am. Relief Agency v. Gonzales,
477 F.3d 728 (D.C. Cir. 2007) 40

Jifry v. FAA,
370 F.3d 1174 (D.C. Cir. 2004) 39

Katz v. Pershing, LLC,
672 F.3d 64 (1st Cir. 2012) 27

Lebron v. Rumsfeld,
670 F.3d 540 (4th Cir. 2012) 23

Legal Tender Cases,
79 U.S. 457, 20 L. Ed. 287 (1870) 31

Lewis v. Cont'l Bank Corp.,
494 U.S. 472 (1990) 18

Mathews v. Eldridge,
424 U.S. 319 (1972) 33

McBryde v. Comm. to Review Circuit Council Conduct & Disability Orders of Judicial Conference of U.S.,
264 F.3d 52 (D.C. Cir. 2001) 23, 24

McConnell v. FEC,
540 U.S. 93 (2003), *overruled on other grounds by*, *Citizens United v. FEC*,
558 U.S. 310 (2010) 15

Morrissey v. Brewer,
408 U.S. 471 (1972) 33

Motor Vehicle Mfrs. Ass'n of the U.S., Inc. v. State Farm Mut. Auto. Ins. Co.,
463 U.S. 29 (1983) 39

Munaf v. Geren,
553 U.S. 674 (2008) 27

Nat. Res. Def. Council, Inc. v. EPA,
22 F.3d 1125 (D.C. Cir. 1994) 16

Nat'l Res. Def. Council, Inc. v. Pena,
972 F. Supp. 9 (D.D.C. 1997) 44

Nat'l Shooting Sports Found., Inc. v. Jones,
716 F.3d 200 (D.C. Cir. 2013) 39

Nat'l Wrestling Coaches Ass'n v. Dep't of Educ.,
366 F.3d 930 (D.C. Cir. 2004) 17

Nken v. Holder,
556 U.S. 418 (2009) 43

O'Bannon v. Town Court Nursing Ctr.,
447 U.S. 773 (1980) 31

Oryszak v. Sullivan,
565 F. Supp. 2d 14 (D.D.C. 2009) 39

Palestine Info. Office v. Shultz,
674 F. Supp. 910 (D.D.C. 1987), *aff'd*, 853 F.2d 932 (D.C. Cir. 1988) 44

Paracha v. Obama,
194 F. Supp. 3d 7 (D.D.C. 2016), *aff'd sub nom*,
Paracha v. Trump, 697 F. App'x 703 (D.C. Cir. 2017) 23

Penthouse Int'l, Ltd. v. Meese,
939 F.2d 1011 (D.C. Cir. 1991) 23, 27

People's Mojahedin Org. of Iran v. Dep't of State,
327 F.3d 1238 (D.C. Cir. 2003) 29

People's Mojahedin Org. of Iran v. U.S. Dep't of State,
182 F.3d 17 (D.C. Cir. 1999) 41

Physician's Education Network, Inc. v. Department of Health, Education & Welfare,
653 F.2d 621 (D.C. Cir. 1981) 16

Qualls v. Rumsfeld,
357 F. Supp. 2d 274 (D.D.C. 2005) 28, 43

Ralls Corp. v. Comm. on Foreign Inv. in the U.S.,
758 F.3d 296 (D.C. Cir. 2014) 34

Regan v. Wald,
468 U.S. 222 (1984) 39, 44

Renal Physicians Ass'n v. U.S. Dep't of Health & Human Servs.,
489 F.3d 1267 (D.C. Cir. 2007) 17, 19, 24, 25

Renne v. Geary,
501 U.S. 312 (1991) 16

Scenic Am., Inc. v. U.S. Dep't of Transp.,
836 F.3d 42 (D.C. Cir. 2016) 17

Secretary of Labor v. Twentymile Coal Co.,
456 F.3d 151 (D.C. Cir. 2006) 38

Serv. Emps. Int'l Union Health & Welfare Fund v. Philip Morris Inc.,
249 F.3d 1068 (D.C. Cir. 2001) 25

St. John's United Church of Christ v. FAA,
520 F.3d 460 (D.C. Cir. 2008) 17

Steel Co. v. Citizens for a Better Env't,
523 U.S. 83 (1998) 25

Texas v. E.P.A.,
726 F.3d 180 (D.C. Cir. 2013) 16

Transp. Workers Union of Am., AFL-CIO v. Transp. Sec. Admin.,
492 F.3d 471 (D.C. Cir. 2007) 16

Travis v. U.S. Dep't of Health & Human Servs,
2005 WL 589025 (D.D.C. Mar. 10, 2005) 26

U.S. Ecology, Inc. v. Dep't of the Interior,
231 F.3d 20 (D.C. Cir. 2000) 17

Wash. Metro. Area Transit Comm'n v. Holiday Tours, Inc.,
559 F.2d 841 (D.C. Cir. 1977) 43

Watervale Marine Co. v. United States Dep't of Homeland Sec.,
55 F. Supp. 3d 124 (D.D.C. 2014), *aff'd on other grounds sub nom*,
807 F.3d 325 (D.C. Cir. 2015) 36, 37

Welborn v. Internal Revenue Serv.,
218 F. Supp. 3d 64 (D.D.C. 2016) 21, 37

Whitaker v. Thompson,
248 F. Supp. 2d 1 (D.D.C. 2002) 43

White v. United States,
601 F.3d 545 (6th Cir. 2010) 16

Wilkinson v. Austin,
545 U.S. 209 (2005) 33

Winpisinger v. Watson,
628 F.2d 133 (D.C. Cir. 1980) 25, 26

Winter v. Nat. Res. Def. Council,
555 U.S. 7 (2008) 27, 43

Wis. Gas Co. v. FERC,
758 F.2d 669 (D.C. Cir. 1985) 42, 43

Zevallos v. Obama,
793 F.3d 106 (D.C. Cir. 2015) 41

STATUTES

5 U.S.C. § 701 ..... 35, 36

5 U.S.C. § 704 36

5 U.S.C. § 706 39

44 U.S.C. §§ 3551-3558 4

44 U.S.C. § 3552 ..... 1, 5, 36, 37

44 U.S.C. § 3553 ..... 1, 5, 13, 37

RULES

Local Civ. R. 65.1 40

REGULATIONS

48 C.F.R. § 9.405 30

48 C.F.R. § 9.406-3 30

National Protection and Programs Directorate; Notifications of Issuance of Binding Operational Directive 17-01 and Establishment of Procedures for Responses,
82 Fed. Reg. 43,784 (Sept. 19, 2017) 12

OTHER AUTHORITIES

163 Cong. Rec. S3492 (2017) 8

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) 8

Disinformation: A Primer in Russian Active Measures and Influence Campaigns,
115th Cong. (2017) 7

Hearing on Worldwide Threats Before the S. Select Comm. on Intelligence,
115th Cong. (May 11, 2017) 8

H.R. 2810,
115th Cong. (2017) 8

H.R. Con. Res. 47,
115th Cong. (2017) 8

S. 1519,
115th Cong. (2017) 8

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 "known or reasonably suspected information security threats, vulnerabilities, or risks." 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 rebut her concerns. Those concerns, reduced to their essence, were that Russia could use Kaspersky software on U.S. information systems as an entry point for espionage or other cyber activities. Russia is a sophisticated adversary that has proven willing and able to compromise and exploit access to U.S. networks, and its intelligence services have an unusually close relationship with Kaspersky and virtually unbounded authority under

Russian law to compel information stored on the company's Russian servers and 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 had to address.

Kaspersky Lab, Inc. and its affiliate, Kaspersky Labs Ltd. (collectively, "Kaspersky"), have now brought this emergency motion for a preliminary injunction to overturn the BOD. They do so more than four months after DHS issued the BOD, and more than a month after Congress effectively codified its prohibition in the National Defense Authorization Act for Fiscal Year 2018 (NDAA). The NDAA imposes a comprehensive, government-wide ban on the use of Kaspersky services and products, 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 for the same reason, Kaspersky does not challenge that statute here. For the reasons set forth below, this Court should deny the request for a preliminary injunction because Kaspersky cannot demonstrate its entitlement to that extraordinary remedy.

As a threshold matter, Kaspersky does not have 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 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. Nothing of any practical value would come from a favorable ruling here, 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 claims also fail on the merits. The company cannot prevail on its claim that DHS denied it due process. Kaspersky's due process arguments exaggerate the process to which it was constitutionally entitled and undervalue the process it actually received. Kaspersky's own account shows that DHS went above and beyond what is procedurally required, including providing the company adequate opportunity to review the agency's grounds and submit information in opposition before DHS 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 a full administrative proceeding before DHS issued the BOD – that is, before DHS took an *initial* action, which, were it to become final, could affect its legal rights.

The company's APA claim fares no better. Kaspersky is not the first private litigant to attempt to use the APA to police a federal agency's actions under the Federal Information Security Modernization Act of 2014 (FISMA). Since FISMA's enactment, numerous 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 FISMA 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 precedents. And even if APA

review were appropriate here, the record amply supports DHS's determination that the removal of the Kaspersky software was necessary to address risks to federal information systems.

In any event, Kaspersky has failed to establish any of the other requirements necessary to obtain a preliminary injunction. The company cannot show that it will suffer irreparable harm in the absence of preliminary relief. Nor can it fairly trace its alleged reputational or commercial harm to the BOD—and even if it could, those harms will remain irreparable so long as the NDAA ban is in place. Kaspersky's burden is even higher in this case because it seeks a mandatory injunction that alters the status quo: it asks the Court to suspend a DHS directive that already has been issued and implemented. This kind of ultimate relief in the guise of a preliminary injunction is disfavored in this circuit and cannot be justified by Kaspersky in this case.

Finally, the balance of equities and the public interest weigh overwhelmingly in favor of the government, which has a strong interest in protecting its information security and maintaining the ability to effectively counter cyber threats. The entire purpose of the BOD is to allow swift and effective action against the real and continuing threat to national security posed by malicious cyber activity. That purpose would be thwarted if courts were willing to second-guess the discretionary judgments of the Secretary and force the government to permit use of software the Secretary has determined poses an unacceptable risk. Kaspersky's motion should be denied.

BACKGROUND

I. 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 own authorities as well as monitoring agencies 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).

Among other cybersecurity tools, Congress authorized the Secretary of DHS to issue compulsory direction to agencies, 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 is authorized to 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 ("safeguarding federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk"), the Secretary has complete discretion to determine when to exercise the BOD authority.

II. Factual Background

a. Kaspersky's Software and Connections to Russia

When an enterprise (in this case, an agency) downloads Kaspersky's antivirus software and consents to the license agreement, it gives the software high-level privileges and broad access to

files on the systems using it. 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 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 dangerous in the wrong hands. If the Russian government were able to exploit Kaspersky's access to U.S. networks, our nation's security could be gravely compromised. Russian agents could install malicious code under the guise of a security update, 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 longstanding 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 767-68, 11-12. 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, 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, 10-11. 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, 11.

The prospect that Kaspersky would be willing to facilitate a Russian cyberattack is not the only concern. Russia has the tools to use Kaspersky software as a platform for espionage whether or not the company is willing to cooperate. Russian law requires the FSB to collaborate with private firms in carrying out its operations, and private firms are legally obligated to assist the FSB in executing its intelligence activities. Further, companies like Kaspersky are required to give the FSB access to user data and install software and equipment that enables the FSB to monitor data transmissions between the company and its users. AR 765-68, 779-87, 14-16.

b. 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 indication 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 Rubio asked a panel of cybersecurity experts if they would feel comfortable using Kaspersky products on their own devices.[2] The

[1] *See, e.g.*, *Russia's Top Cyber Sleuth Foils US Spies, Helps Kremlin Pals*, Wired (July 23, 2012), https://www.wired.com/2012/07/ff_kaspersky/all/

[2] *Disinformation: A Primer in Russian Active Measures and Influence Campaigns*, 115th Cong. 41 (2017)

following month, the U.S. Senate Select Committee on Intelligence asked the Director of National Intelligence and the Attorney General to investigate the company's ties to the Russian government,[3] and two House Democrats 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 networks. NSA Director Mike Rogers noted that he was "personally involved" in monitoring the Kaspersky issue.[5]

In the ensuing months, lawmakers and regulators began taking more concrete actions to address concerns about Kaspersky software. In June, Senator Cotton proposed an amendment to an Iran sanctions bill that called for the imposition of mandatory economic sanctions against Kaspersky employees in Russia.[6] 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.[7] Later that month, Senator Shaheen filed an amendment to the House version of the NDAA to prohibit the use of Kaspersky software government-wide.[8] In support of the amendment,

---

[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) (opening statement of Rep Beyer), available at https://democrats-science.house.gov/sites/democrats.science.house.gov/files/documents/10.25.17%20RM%20Beyer%20Opening%20Statemenet%20Kaspersky%20Lab%20Products%20Hearing_0.pdf

[4] H.R. Con. Res. 47, 115th Cong. (2017)

[5] *Hearing on Worldwide Threats Before the S. Select Comm. on Intelligence*, 115th Cong. (May 11, 2017)

[6] 163 Cong. Rec. S3492 (2017)

[7] S. 1519, 115th Cong. (2017)

[8] Amendment (SA 663) to the House NDAA (H.R. 2810, 115th Cong. (2017))

Senator Shaheen cited "alarming and well-documented" ties between Kaspersky and the Kremlin.[9] Around this time, Representative Lamar Smith, Chairman of the U.S. 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 starting 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 with the Russian government had attracted extraordinary publicity. While the bulk of these reports focused on increasing scrutiny from the federal government, a number of stories purported to bring new information to light, including a July 2017 Bloomberg report that Kaspersky has a much closer relationship to Russian intelligence services than the company had previously admitted.[10] These reports contributed 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,

---

[9] Press Release, Senator Jeanne Shaheen, Shaheen's Legislation to Ban Kaspersky Software Government-Wide Passes Senate As Part of Annual Defense Bill (Sept. 18, 2017), https://www.shaheen.senate.gov/news/press/shaheens-legislation-to-ban-kaspersky-software-government-wide-passes-senate-as-part-of-annual-defense-bill-

[10] Cyrus Farviar, *Kaspersky under scrutiny after Bloomberg story claims close links to FSB*, Ars Technica (July 11, 2017), https://arstechnica.com/information-technology/2017/07/kaspersky-denies-inappropriate-ties-with-russian-govt-after-bloomberg-story/.

with sources familiar with the decision attributing it to concerns over the company's ties to Russian intelligence services.[11]

c. 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 633-35. 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. *Id*.

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.[12] AR 629, 753. That

---

[11] Reuters Staff, *Best Buy stops sale of Russia-based Kaspersky products*, Reuters (Sept. 8, 2017), https://www.reuters.com/article/us-usa-kasperskylab-best-buy/best-buy-stops-sale-of-russia-based-kaspersky-products-idUSKCN1BJ2M4

[12] 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'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*

decision, 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 the Assistant Secretary for Cybersecurity and Communications (AR 3-24, 752-76), 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 National Cybersecurity and Communications Integration Center ("NCCIC") (AR 25-32, 822-32), as well as an expert opinion 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 639-46. The administrative process was designed to ensure that Kaspersky and other parties would have a reasonable amount of time to prepare a response, leaving the Acting Secretary with the remaining time to consider any information submitted and provide a response before reaching a final decision at the 90-day mark. This feature of the process was noted in the BOD, which stated that the 90-day start of

---

information, a meaningful adjudication of Kaspersky's claims can occur without DHS and the Court needing to address the impact of national security information on this case.

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 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. 82 Fed. Reg. 43,784. 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 647-683.

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 755-56. 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 755. 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 756.

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 756-57.

In total, fourteen agencies identified Kaspersky-branded products on their information systems. AR 757. 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*.

d. 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.

The NDAA ban requires that all agencies have discontinued use of Kaspersky products and services by October 1, 2018, the first day of the new fiscal year. NDAA § 1634(a). In the meantime, Congress directed DOD, in consultation with various federal 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 a description of 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.[13]

To establish standing to sue in federal court, 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. Bentson,* 94 F.3d 658, 663 (D.C. Cir. 1996) (citations omitted). Redressability requires "that it be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." *Chamber of Commerce v. EPA,* 642 F.3d 192, 201 (D.C. Cir. 2011) (citation omitted). In a case like this, where "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); *see Dynatlantic Corp. v. Dep't of*

[13] In light of this jurisdictional deficiency, this Court can dismiss the Complaint on its own motion. *Akinseye v. D.C.*, 339 F.3d 970, 971 (D.C. Cir. 2003). The government also is prepared to move to dismiss the Complaint on this ground, among others, following the Court's decision on the present motion, should the Court so desire.

Def, 115 F.3d 1012, 1017 (D.C. Cir. 1997) ("redressability and traceability overlap as two sides of a causation coin").

This case turns principally on the absence of these related elements.[14] Kaspersky identifies the injury it has suffered as loss of the firm's "substantial interest in its status as a vendor to the U.S. Government." Compl. ¶ 34, ECF No. 1. According to Kaspersky, this injury includes both the loss of the ability to sell its products to the U.S. government and the purported damage to the company's reputation and attendant commercial harm. Prelim. Inj. Mem. ("PI Memo") at 10-14, ECF No. 10. It is Kaspersky's burden to show that its injury is "likely" traceable to the challenged action and redressable by the requested relief. *Chamber of Commerce*, 642 F.3d at 201. Kaspersky has not carried that burden here. Where, as here, an unchallenged law causes the same injury as the action being challenged, a court is powerless to provide effective relief. As long as the NDAA ban is in place, Kaspersky has nothing to gain from winning here.

a. Kaspersky's Loss of Its "Status as a Vendor" Is Not Redressable Because the NDAA Ban Forecloses Any Effective Judicial Relief from the Alleged Injury.

The redressability problem in this case is a textbook example of the familiar rule that standing does not exist where an independent constraint forecloses an effective remedy. In this line of cases, standing fails not because the prospect of relief is too speculative or remote, but rather because it is legally or practically foreclosed by forces outside the court's control. *See, e.g.*, *McConnell v. FEC*, 540 U.S. 93 (2003) (striking down increases in campaign contribution limits would not redress the alleged injury because the limitations imposed by a separate, unchallenged provision of the statute would remain the same), *overruled on other grounds by Citizens United v.*

[14] Although the standing deficiencies discussed below also could be framed in terms of traceability, for clarity and to avoid repetition, this analysis discusses them principally in terms of redressability.

FEC, 558 U.S. 310 (2010). Thus, where two laws independently cause the same injury, a plaintiff lacks standing to challenge only one of them. *See, e.g.*, *Delta Const. Co. v. EPA*, 783 F.3d 1291, 1296 (D.C. Cir. 2015). The plaintiffs in *Delta*, for instance, claimed they had standing to challenge an EPA pollution standard because it increased the price of the vehicles they bought. Those vehicles, however, also were subject to "substantially identical" pollution standards established by the National Highway Traffic Safety Administration. Because "both [agencies' standards], jointly, are the source of [higher vehicle costs]," vacating one agency's standards while leaving the other's in place would do nothing to redress the alleged harm. *Delta*, 783 F.3d at 1296;[15] *see Physician's Education Network, Inc. v. Department of Health, Education & 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).[16]

---

[15] *See also Texas v. E.P.A.*, 726 F.3d 180, 199 (D.C. Cir. 2013) (where statute, not challenged rule, caused states' inability to issue permits, states' challenge to rule was not redressable); *Transp. Workers Union of Am., AFL-CIO v. Transp. Sec. Admin.*, 492 F.3d 471, 477 (D.C. Cir. 2007) (no standing to challenge TSA rule where vacating the challenged rule would leave in place a previous version of the rule that would cause the same injury); *Nat. Res. Def. Council, Inc. v. EPA*, 22 F.3d 1125, 1147 (D.C. Cir. 1994) ("NADA therefore is hard pressed to claim that it was injured by the rulemaking because, as discussed above, it is the statute, rather than the form of the guidance, which requires states to "comply in all respects" with the EPA's guidance and authorizes the Administrator to impose sanctions on nonattaining states"); *cf Renne v. Geary*, 501 U.S. 312, 319 (1991) (finding a dispute nonjusticiable where another unchallenged statute "might be construed" to prohibit the same conduct as the challenged statute).

[16] Numerous decisions from outside this circuit affirm this reasoning. See *Drakes Bay Oyster Co. v. Jewell*, 747 F.3d 1073, 1092 (9th Cir. 2014) (plaintiff seeking to use estuary for oyster farm lacked standing to challenge notice of wilderness designation, where Secretary of Interior had already denied permit to operate); *White v. United States*, 601 F.3d 545, 552 (6th Cir. 2010) (plaintiff lacked standing to challenge a federal ban on cockfighting where the same conduct was uniformly banned throughout the states); *Advantage Media, LLC v. City of Eden Prairie*, 456 F.3d 793 (8th Cir.2006) (a favorable decision would not allow plaintiff to build desired sign where the sign would still violate unchallenged provisions of the sign code).

This principle is not confined to cases where two laws independently 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 by the plaintiff, that 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. Dep't 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 St. John's United Church of Christ v. FAA*, 520 F.3d 460, 463 (D.C. Cir. 2008) (where a plaintiff challenged a federal grant to reimburse city for airport improvement projects on the theory that the projects could not be completed without federal money, redressability could not be shown because the city was committed to completing the project with or without federal funding).[17]

These precedents compel the conclusion that the NDAA ban eliminates any possibility of effective judicial relief. As in *Physicians*, *Delta*, and similar cases, an unchallenged law, here section 1634(a) of the NDAA, proscribes the same conduct as the agency action Kaspersky seeks

[17] *See also Scenic Am., Inc. v. U.S. Dep't of Transp.*, 836 F.3d 42, 45 (D.C. Cir. 2016) (no standing to challenge federal agency's interpretation of statutory prohibition on billboards where there was no evidence that a favorable ruling would cause local division offices to prevent the states they oversee from erecting digital billboards); *U.S. Ecology, Inc. v. Dep't of the Interior*, 231 F.3d 20, 25 (D.C. Cir. 2000) (developer who sought to build waste facility on federal land lacked standing to challenge the U.S. government's decision not to approve sale of the proposed development site to California because redress was contingent on California's independent decision whether or not to accept title to the land).

to enjoin, rendering the court powerless to abate the company's purported injury from the loss of its "status as a vendor." Rescinding the BOD would leave the full machinery of the congressional ban in effect, which means federal agencies would still face a binding directive to discontinue the use of Kaspersky software by October 1, 2018, including reporting in the interim on "the authorities and procedures for removal of suspect products." NDAA § 1634(c). The court could not redress the legal component of Kaspersky's injury because 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. And 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 congressional ban, which 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), and which puts the force of Congress's legislative power behind a determination that the company's products are not safe for federal networks.[18]

[18] This conclusion applies with equal, if not greater force to Kaspersky's request for declaratory relief. The Court's authority to issue declaratory relief extends only to the resolution of actual controversies; it does not permit the Court to render advisory opinions on "abstract disagreement[s]" about the validity or invalidity of provisions of law. *Lewis v. Cont'l Bank Corp.*, 494 U.S. 472, 479 (1990). If enjoining the BOD cannot redress the legal component of Kaspersky's injury, then a bare declaration of its invalidity would fare no better, particularly if that decision were based on something other than the merits. It would be nothing but an advisory opinion for this court to evaluate the lawfulness of DHS's action when the court's assessment cannot redress the alleged injury.

It makes no difference, for purposes of standing, that the prohibition in the NDAA does not take effect until later this year. Even without being in force, the ban would still "hold 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 breadth of the ban suggests that Congress was contemplating 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 reporting requirements shows that Congress assumed implementation efforts would begin immediately.[19] Congress has spoken on the use of Kaspersky products, and its intent was clear. In these circumstances, no agency would even contemplate purchasing Kaspersky products if this Court granted relief, and rescinding the BOD would not restore Kaspersky's "status" as government vendor.

i. Any Harm Stemming from Kaspersky's Inability to Sell to the United States Is Not Redressable.

As explained above, the NDAA ban forecloses any meaningful relief for the general injury Kaspersky alleges in its Complaint – loss of status as a vendor. The first component of this purported injury, the loss of Kaspersky's ability to sell its products to the U.S. government, fails for the same reason. In these circumstances, where federal agencies are required to stop using

[19] Congress's desire for swift action is reinforced by the provision's reporting requirements, which give the Secretary of Defense, in consultation with other agencies, until June 2018 to review and report on a host of issues concerning the "procedures for removing suspect products or services." Section 1634(c)(1). Although the statute does not specifically call for reporting about the removal of Kaspersky products, the placement of the reporting provision and its general subject matter leave little doubt that Congress was contemplating reporting on the implementation of the Kaspersky ban. As such, the provision presupposes that agencies would have implementation experience relevant to the June report, and that they would not be biding their time until the ban takes effect in October.

Kaspersky products by October 1 and report on their progress in the interim, both common sense and the realities of federal procurement policy 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 declaration of Grant Schneider, the Federal Chief Information Security Officer (CISO), reinforces that conclusion. *See* Declaration of Grant Schneider, Federal CISO ("Schneider Decl."), Exhibit 1. As Federal CISO and a former agency Chief Information Officer (CIO), 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 it would be impossible for a procurement official to justify the security risks and acquisition costs associated with a short-term investment in Kaspersky software.

With respect to costs, Schneider concludes that it would be "inexcusably wasteful" for an agency to purchase software knowing that federal law will soon prohibit its use. *Id*. ¶ 9. Having recently taken steps to remove Kaspersky-branded software from their information systems (or taking steps to confirm that they were not using the software in the first place), and having begun to prepare for the arduous task of combing their hardware and software for traces of Kaspersky code, no agency would make an investment in Kaspersky software and go to the trouble of testing, installing, and integrating the software, only to have to remove it and start the process anew within a matter of months. *See id*. ¶¶ 9-11. Substituting one antivirus solution on an agency network for another normally requires considerable money and resources, above and beyond the cost of licensing the software. *Id*. ¶ 9. In addition to the costs of testing, installation, and obtaining the

necessary permissions,[20] there are the costs of purchasing software without the benefit of the GSA schedule contract, *see* AR 559-61, and the wasted expense of paying the price of a one-year license for software it can use only for a matter of months. To make matters worse, the agency would be incurring these costs twice—once after the software becomes temporarily lawful and again when the NDAA ban takes effect.

Even if agencies were inclined to ignore these issues, they still would need to make the independent judgment that the benefits of using Kaspersky's products outweigh the security risks. *Welborn v. Internal Revenue Serv.*, 218 F. Supp. 3d 64, 81 (D.D.C. 2016) ("[E]ach agency head is delegated full discretion in determining how to achieve [FISMA's] goals, which removes it from APA review."). But acquiring Kaspersky software in these circumstances would make even less sense from a risk-management standpoint. While a court-ordered rescission of the BOD would remove an immediate (albeit temporary) legal barrier to acquiring the software, it would not erase the security concerns underlying DHS's decision to issue the BOD, GSA's decision to remove Kaspersky from its contract schedules, and, ultimately, Congress's decision to impose a government-wide ban on Kaspersky products. Given the publicly available evidence and the consensus among lawmakers and intelligence officials, Schneider CIO concludes understandably that "if I was still an agency CIO, I could not reasonably accept the risk presented by the installation of Kaspersky products on my agency's information systems, and I find it highly unlikely that any other official would make a contrary decision." Schneider Decl. ¶ 7.

[20] Agencies are required to complete an "Authorization to Operate" before using an information system operationally and to conduct a reauthorization when the agency intends to make a change "likely to affect the security or privacy state of an information system." *See* OMB Circular A-130 at Appendix I-7, I-21 – I-22. Based on Mr. Schneider's knowledge and experience, substituting one anti-virus solution for another across an enterprise is a change that is likely to affect the security or privacy state of an information system. Schneider Decl. ¶ 10.

The bottom line is that Kaspersky's inability to sell products to the United States 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.

With the NDAA ban impending, the most Kaspersky could hope for is a narrow window, likely no more than several months, during which an agency could acquire 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). The abstract vindication Kaspersky would get from seeing the BOD overturned is not sufficient under Article III. *See Int'l Union of Bricklayers & Allied Craftsmen v. Meese*, 761 F.2d 798, 802 (D.C. Cir.1985) ("Not all that which may befall an individual is amenable to judicial correction; an abstract 'injury' will find no relief in federal court."); *Huntington Branch, N.A.A.C.P. v. Town of Huntington*, 689 F.2d 391, 394 (2d Cir. 1982) ("To be sure, those who have absolutely no realistic financing capability have no standing, because, as to them, invalidation of an offending ordinance would afford only moral satisfaction rather than a realistic opportunity to proceed with construction." (citations omitted)).

ii. 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.

With respect to redressability, Kaspersky's reputational injury suffers from the same basic deficiencies as the loss of its ability to sell products to the U.S. government. Rescinding the BOD

would not relieve Kaspersky's asserted reputational harm because there still would be law branding Kaspersky software as a security risk and effectively excluding the company from doing business with the U.S. government. The NDAA imposes a government-wide prohibition on the use of Kaspersky products and services, based on a legislative judgment that the company's software cannot be used on federal systems without an unacceptable risk of exploitation. 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). 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); *cf Penthouse Int'l, Ltd. v. Meese*, 939 F.2d 1011, 1019 (D.C. Cir. 1991) (declaring that a since-withdrawn letter violated the plaintiff's First Amendment rights would not likely redress any reputational injury not already remedied by the withdrawal).

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 even more obvious in this context, because there can be no question as to whether the harmful reputational effects of the NDAA occurred immediately (as opposed to October 1, when it takes effect), and because there are other forces, in addition to the NDAA ban, that are working to hold the new status quo place. Those forces, discussed further below, include the removal of Kaspersky from GSA's contract schedules, and the countless other statements, government actions, and press reports that have contributed to the company's notoriety.

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 Acting Secretary's decision to issue the BOD. That assumption is wrong: as explained below, *see, infra* II.a.ii., 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 BOD on the merits 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 lacks authority to pass judgment on the merits of the underlying action. *See McBryde*, 264 F.3d at 57 (the court "could not see how" a declaration that a Judicial Council had acted *ultra vires* in suspending a district 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, whether in connection with an injunction or

through a declaratory judgment, 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, "they were banned by the US from use in all federal agencies," PI Memo at 11, 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 the DHS action" would be willing to reengage in a world where the BOD were gone but the NDAA remained law, Gentile Decl. ¶ 23.

Redressability aside, Kaspersky cannot show that its purported harm is fairly traceable to the BOD, as opposed to the actions of third parties not before the Court. Dismissal at the pleadings stage for lack of standing is appropriate where, as here, the alleged injuries are speculative and difficult to ascertain in light of other causes. *See, e.g., Serv. Emps. Int'l Union Health & Welfare Fund v. Philip Morris Inc.*, 249 F.3d 1068, 1073-74 (D.C. Cir. 2001). Indeed, 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. Kaspersky's alleged reputational harm is not fairly traceable to the BOD, as opposed to the "endless number of diverse factors potentially contributing" to it.

Winpisinger, 628 F.2d at 139. 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, at least two 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." Gentele Decl. ¶ 20, ECF No. 10-2. 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 11.

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.[21]

II. Kaspersky Is Not Entitled to a Preliminary Injunction

A preliminary injunction is an "extraordinary and drastic remedy" that is "never awarded as of right." *Munaf v. Geren*, 553 U.S. 674, 689-90 (2008) (citations omitted). A preliminary injunction "may only be awarded upon a clear showing that the plaintiff is entitled to such relief." *Winter v. Nat. Res. Def. Council*, 555 U.S. 7, 22 (2008). "A plaintiff seeking a preliminary injunction must establish that he is likely to succeed on the merits, that he is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in his favor, and that an injunction is in the public interest." *Id.* at 20; *Abdullah v. Obama*, 753 F.3d 193, 197

[21] 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).

(D.C. Cir. 2014). Further, in a case like this, where "the injunction sought would alter, rather than preserve, the status quo," the plaintiff must meet an even higher standard: he must demonstrate "a clear entitlement to relief" or that "extreme or very serious damage will result if the injunction does not issue." *Qualls v. Rumsfeld*, 357 F. Supp. 2d 274, 279 (D.D.C. 2005). For the reasons discussed below, Kaspersky cannot meet this heavy burden.

a. Kaspersky Is Unlikely To Prevail on the Merits

As explained, Kaspersky is unlikely to prevail because this Court lacks jurisdiction to consider its claims. But if the Court had jurisdiction, Kaspersky's claims would still fail on the merits.

i. Kaspersky Has Failed to State a Procedural 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, but was gathering information during that period and reserved the 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 advanced 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).[22] 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 contend that it was denied an opportunity to provide relevant information in opposition to 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 principal grievance is that DHS should have notified the company sooner, before taking action that effected an "immediate debarment" of Kaspersky Lab from government business. PI Memo 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 this deprivation, the company asserts, is constitutionally deficient. According to Kaspersky, a "meaningful" process would have mirrored the pre-deprivation procedures used for the suspension and debarment of federal contractors. PI Memo at 25. As explained below, debarment is not an appropriate model for evaluating the due process claim in this case, and Kaspersky's analogy to debarment procedures overstates the process to which it was constitutionally entitled. But 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.

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

[22] 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).

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. PI Memo at 25. As with the debarment process, the BOD provided Kaspersky with prompt notice of the action being considered; a thorough summary 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 their 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 or 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 order removal. 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.[23] *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").

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

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

As set forth above, the pre-deprivation process afforded to Kaspersky was comparable to, and in some respects greater than, what Kaspersky refers to as the "well-established" and "constitutionally adequate" debarment procedures, and any differences between the two procedures are not of constitutional dimension. Because the administrative process meets the due process benchmark set by Kaspersky, that should end the matter. Nevertheless, 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 Government's interest, including the . . fiscal and administrative burdens that the additional or substitute procedural requirement would entail." 424 U.S. 319, 335 (1972). 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) (quoting *Boddie v. Connecticut*, 401 U.S. 371, 378 (1971)).

Rather than attempting to balance these factors, Kaspersky simply assumes, based solely on the first factor, that it is entitled to the same level of due process protections as any other seller of products facing debarment. It may be that Kaspersky suffered the same practical consequences as such a company, but that does not mean both require the same procedural protections. *Mathews* makes clear that 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. 319, 335; *see also Morrissey v. Brewer*, 408 U.S. 471 (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 Wilkinson v. Austin*, 545 U.S. 209, 224 (2005).

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"). That interest should weigh heavily in the balance, more so than the government's interests in the debarment context, where the most immediate concern is curbing fraud and waste. *See Caiola v. Carroll*, 851 F.2d 395, 398 (D.C. Cir. 1988) ("Debarment reduces the risk of harm to the system by eliminating . . . the unethical contractor").

Further, Kaspersky's private interests are well protected by the government's existing 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 BOD achieves this by ensuring that the government is accounting for all relevant information and that aggrieved parties have an opportunity to draw the government's attention to any possible errors. There is no reason that providing process earlier could yield a different result, particularly in light of the sensitivity of the underlying information and the discretionary nature of the threat assessments at issue.

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 *prevent any chance of* cyber intrusions – not, as Kaspersky suggests, to *conclusively prove* them. FISMA is not a criminal statute that requires proof someone has committed a security breach or violated a security standard; rather, it is a risk-avoidance provision that requires only the *possibility* of danger. 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.

Under these circumstances, 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.

3. Kaspersky Was Not Constitutionally 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. PI Memo at 30. 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 discussed, among other authorities and levers of political influence, the FSB's authority to compel assistance from Russian companies 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 specific 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 thorough, 21-page summary 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 could and 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 their statutory authority and threatening their core missions.

ii. Kaspersky Has Failed to State a Claim under the Administrative Procedures Act

Kaspersky's APA claim fails at the threshold. The APA precludes judicial review where, as here, "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, Kaspersky cannot show any likelihood of success on the merits of its APA claims.

The Department'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). The Supreme Court has explained that 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) (citation omitted). In making this assessment, the D.C. Circuit considers a variety of factors, which fall into three principal categories: (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. United States Dep't of Homeland Sec.*, 55 F. Supp. 3d 124, 137-38 (D.D.C. 2014) (internal 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 pursuant to 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*. Instead, Congress has vested complete discretion in the Secretary to make judgments about cyber threats that may warrant invocation of the BOD authority. Notably, 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," demonstrates Congress's deference to the Secretary and its recognition of the Secretary's 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. 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*, 218 F. Supp. 3d at 81. The deferential approach reflected in the statutory scheme, in which "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.*, 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."), *appeals filed* Nos. 17-5217 (D.C. Cir. 2017), 17-5232 (D.C. Cir. 2017), *sub. nom. AFGE, AFL-CIO v. OPM*, No. 18-1182 (Fed. Cir. 2017); *Welborn*, 218 F. Supp. 3d at 81. 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).

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. *Secretary 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 action involves the review and analysis of sensitive, potentially classified intelligence, coupled with the understanding and analysis of an ever-evolving cybersecurity environment. Further, the information and analysis underlying these 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 America, Inc. v. Browner*, 83 F.3d 445, 452 (D.C. Cir. 1996) (citations omitted). That is especially true in this context, 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 akin to the decision to grant or deny an individual's security clearance – a

decision which the courts have recognized is "committed to agency discretion." 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. 2009), applies equally here.

Even if the court were to conclude that the decision was 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 "(A) arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law; (B) contrary to constitutional right, power, privilege, or immunity; (C) in excess of statutory jurisdiction, authority, or limitations, or short of statutory right; [or] (D) without observance of procedure required by 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; *Motor Vehicle Mfrs. Ass'n of the U.S., Inc. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983). The agency's decision should be affirmed as long as it is supported by a rational basis. *See Motor Vehicle Mfrs. Ass'n*, 463 U.S. at 43; *Nat'l Shooting Sports Found., Inc. v. Jones*, 716 F.3d 200, 214 (D.C. Cir. 2013); *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) ("we 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 heavily deferential standard accorded 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; and (2) failed to present "conclusive evidence that Kaspersky Lab had facilitated any breach of U.S. national security."[24] Pl Mem. at 32-33. Neither argument has merit.

There is no merit to Kaspersky's contention that DHS improperly relied on news reports, purportedly at the expense of "meaningful[] . . . agency fact-finding." PI Memo at 32. To the extent Kaspersky contends there was something procedurally improper about relying on news

[24] The complaint includes several additional arguments concerning the judgments the Acting Secretary drew from the evidentiary record. Compl. ¶¶ 64-74. Because those arguments were not raised in the application for preliminary relief, the Court need not consider them at this stage, and the government reserves the right to address them in a later filing. *See* Local Civ. R. 65.1(c) (requiring applications for a preliminary injunction to be made in a document "separate from the complaint"). In any event, most of these arguments seek to question or minimize the Acting Secretary's concerns, without actually contesting the factual ground on which they rest. They amount to little more than disagreement with the Acting Secretary's determination that Kaspersky software presents a risk to federal information systems. But an agency's determination and explanation are not arbitrary or capricious simply because the plaintiff, or the even the court, disagrees with its conclusion. *See, e.g.*, *Huls America Inc.*, 83 F.3d at 452.

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) (noting that "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 ("it 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. PI Memo at 32. The Acting Secretary'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 an expert opinion on relevant aspects of Russian law. 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 does not identify a single report that is inaccurate or unreliable.

Kaspersky repeatedly points out that DHS has presented no evidence of any "breach" or "wrongdoing" on the part of Kaspersky. PI Memo at 33. 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, and is in no way limited to actors that have carried out malicious activity in the past. As long as Kaspersky products were present on federal information systems, the Russian government 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.

III. Kaspersky Will Not Suffer Irreparable Harm Absent a Preliminary Injunction

Kaspersky falls well short of demonstrating a great and certain harm that would be required for preliminary injunctive relief, and its motion should be denied on that basis alone. The only harms Kaspersky claim to be irreparable are reputational damage and financial losses. PI Mem. at 34-36. But for the same reason that Kaspersky cannot demonstrate a redressable injury, it cannot demonstrate that it will suffer irreparable harm in the absence of a preliminary injunction. Similarly, for the same reasons Kaspersky has failed to demonstrate that its reputational and financial harms are fairly traceable to the BOD, as opposed to numerous other government actions that preceded and followed it, it cannot "provide proof" that the financial losses it faces "will *directly result* from the *action* which [Kaspersky] seek[s] to enjoin." *Wis. Gas Co. v. FERC*, 758 F.2d 669, 674 (D.C. Cir. 1985) (emphasis added).[25] Kaspersky faces an especially high burden of

[25] In any event, it is "well settled that economic loss does not, in and of itself, constitute irreparable harm," *Wis. Gas Co.*, 758 F.2d at 674, especially when it is nothing more than speculation about how third parties might respond to government actions.

persuasion here because it seeks to upset, rather than preserve the status quo by suspending a DHS action that already has been issued and implemented. *See Qualls*, 357 F. Supp. 2d at 279.

Kaspersky has not substantiated *any* of the myriad, speculative links in the chains of causation and redressability required for Article III standing, much less tendered proof that would permit this Court to find that the BOD caused an increase in financial losses of sufficient gravity to warrant injunctive relief. *See Winter*, 555 U.S. at 22 ("Issuing a preliminary injunction based only on a possibility of irreparable harm is inconsistent with our characterization of injunctive relief as an extraordinary remedy that may only be awarded upon a clear showing that the plaintiff is entitled to such relief."); *Wis. Gas Co.*, 758 F.2d at 675-76 (finding alleged harm "specious," given "common knowledge" that harm depends on many "variables").

IV. The Balance of Equities Favor the Government.

The final two factors in the standard for preliminary and injunctive relief—the balance of equities and the public interest—tend to "merge" in cases where the relief is sought against the United States. *Nken v. Holder*, 556 U.S. 418, 435, 1 (2009). Kaspersky has failed to demonstrate that "the threatened irreparable injury outweighs the threatened harm that the injunction would cause Defendants and third parties" and that "granting the preliminary injunction would be in the public interest." *Whitaker v. Thompson*, 248 F. Supp. 2d 1, 7-8 (D.D.C. 2002) (citation omitted); *see also Wash. Metro. Area Transit Comm'n v. Holiday Tours, Inc.*, 559 F.2d 841 (D.C. Cir. 1977). On the contrary, the balance of the equities and the public interest weigh heavily against Kaspersky and its request for a preliminary injunction.

The United States has a substantial interest in protecting the integrity of its information systems from cyber threats, and the Secretary's BOD authority was devised by Congress and exercised by DHS in order to accomplish exactly this purpose. Entry of a preliminary injunction

would frustrate action to address a cybersecurity risk that poses a significant threat to the U.S. national security. Courts have generally held that the balance of interests tips sharply in favor of the government when dealing with issues, such as cybersecurity, that touch on foreign policy and national security. *See Adams v. Vance*, 570 F.2d 950, 954 (D.C. Cir. 1978) (in case touching on foreign policy, "a court is quite wrong in routinely applying to this case the traditional standards governing more orthodox stays." (citation omitted)); *see also Regan*, 468 U.S. at 242 (citing "classical deference to the political branches in matters of foreign policy"); *Palestine Info. Office v. Shultz*, 674 F. Supp. 910, 918 (D.D.C. 1987) (requiring an "exceptionally strong" showing to receive a preliminary injunction), *aff'd*, 853 F.2d 932 (D.C. Cir. 1988). More generally, it is not in the public interest to delay policies that promote public safety, national security, and administrative efficiency, as Kaspersky seeks to do here. *See, e.g.*, *Nat'l Res. Def. Council, Inc. v. Pena*, 972 F. Supp. 9, 20 (D.D.C. 1997); *Hodges v. Abraham*, 253 F. Supp. 2d 846, 873 (D.S.C. 2002); *Gulf Oil Corp. v. Fed. Energy Admin.*, 391 F. Supp. 856, 864 (W.D. Pa. 1975).

Finally, it is neither the role of the Court nor the purpose of a preliminary injunction to dictate policy in the area of national security or foreign relations. The Supreme Court has repeatedly 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; *see also Regan*, 468 U.S. at 242; *Harisiades v. Shaughnessy*, 342 U.S. 580, 589 (1952) ("Matters related '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 interference."'); *Palestine Info. Office*, 674 F. Supp. at 918; *see also Global Relief Found. v. O'Neill*, 207 F. Supp. 2d 779, 787-88 (N.D. Ill. 2002), *aff'd* 315 F.3d 748 (7th Cir. 2002). 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

For the foregoing reasons, the Court should deny Kaspersky's request for a preliminary injunction.

Dated: February 5, 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
Telephone: (202) 616-8014
Fax: (202) 616-8470