UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

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

MEMORANDUM OF LAW IN SUPPORT OF
PLAINTIFFS' MOTION FOR SUMMARY JUDGMENT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

INTRODUCTION

"[T]he power of debarment is tantamount to one of life or death over a business." *Gonzalez v. Freeman*, 334 F.2d 570, 575 n.5 (D.C. Cir. 1964)(J. Burger)(quotation omitted). The U.S. Department of Homeland Security (DHS) exercised that power against Plaintiffs Kaspersky Lab, Inc. and Kaspersky Labs Limited (collectively, "Kaspersky Lab" or the "Company") on September 13, 2017, when it issued Binding Operational Directive 17-01 ("the BOD"). The BOD explicitly labeled the antivirus software products developed by the Company "information security risks" to U.S. government information systems, summarily ordered their removal from those systems, and followed with a permanent debarment. In doing so, DHS violated the Company's Fifth Amendment procedural due process rights by effectuating an immediate debarment with neither prior notice nor a prior opportunity to contest the purported evidence underlying the BOD. Because the BOD relies principally on media reports (rather than meaningful agency fact-finding) and an insufficient technical assessment, the BOD also violated the evidentiary requirements of the Administrative Procedure Act (APA).

The BOD was issued pursuant to the Federal Information Security Modernization Act of 2014 ("FISMA") 44 U.S.C. § 3551 *et seq*. (2014). That statute authorizes the issuance of a binding operational directive only "for the purposes of safeguarding Federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk." 44 U.S.C.§ 3552(b)(1). In issuing the BOD, DHS explained in its accompanying press release that:

> The BOD calls on departments and agencies to identify any use or presence of Kaspersky products on their information systems in the next 30 days, to develop detailed plans to remove and discontinue present and future use of the products in the next 60 days, and at 90 days from the date of this directive, unless directed otherwise by DHS based on new information, to begin to implement the agency plans to discontinue use and remove the products from information systems.

The BOD professed to provide due process through this 30-60-90 day implementation structure and the opportunity for Plaintiffs to lodge an objection with DHS in the midst of that implementation. However, this process was illusory and did not meet minimum due process standards. In reality, the debarment of Plaintiffs was immediate and complete *upon the issuance* of the BOD on September 13, 2017. As DHS itself explains in its accompanying press release, the BOD "directed" agencies to immediately "take actions" upon issuance of the BOD:

> After careful consideration of available information and consultation with interagency partners, Acting Secretary of Homeland Security Elaine Duke today issued a Binding Operational Directive (BOD) directing Federal Executive Branch departments and agencies to take actions related to the use or presence of information security products, solutions, and services supplied directly or indirectly by AO Kaspersky Lab or related entities. (emphasis added).

All legal determinations (and the relevant administrative decision for the purposes of the APA) had been made by the time that the BOD was issued. DHS's inclusion of a proviso in the BOD—"unless otherwise directed by DHS based on new information"—does not transform the BOD itself into pre-deprivation due process. Upon issuance, the BOD labeled Kaspersky Lab software an "information security risk," and effectively barred agencies from purchasing the software at any point in the future.

Indeed, DHS has publicly acknowledged that agencies began removing software well before the 90-day mark without regard to the purported process set forth by the BOD. The process for identification, removal, and discontinuation began immediately and, alongside private and commercial consumers, unfairly prejudiced government agencies against Plaintiffs' software.

DHS's professed administrative process gave Plaintiffs an opportunity to respond to the BOD only *after* it effected their debarment on September 13, 2017, while the identification and removal of their software was ongoing at federal agencies. Following this process nonetheless

and in good faith, Plaintiffs filed a lengthy written submission with DHS on November 10, 2017, challenging the BOD and attempting to change its result (the "Kaspersky Lab Submission"). Plaintiffs' attempts were futile, as they were destined to be. DHS rejected Plaintiffs' arguments made in the Kaspersky Lab Submission in a "Final Decision" dated December 6, 2017, which maintained the BOD without modification just days ahead of the 90-day mark, which fell on December 13, 2017.

DHS cannot justify the absence of pre-deprivation process here. DHS has never claimed that the alleged "information security risks" cited in the BOD were imminent, exigent, or urgent. Many of the media reports cited by DHS in support of the BOD are several years old, and Plaintiffs' software operates today in much the same way it always has. What has changed in 2017 is the increase in political scrutiny following Russia's apparent interference in the 2016 presidential election, in which there is no allegation that Plaintiffs had any involvement. In issuing the BOD, DHS bowed to that pressure and took hasty action that deprived Plaintiffs of their due process rights. In doing so, DHS has failed to demonstrate Plaintiffs' software presented such an "extraordinary situation" to necessitate the postponement of due process until after the deprivation of a protected interest. *See Boddie v. Connecticut*, 401 U.S. 371, 379 (1971).

Further, rather than DHS using a meaningful fact-finding process, the principal and overwhelming source of "evidence" underlying the BOD is uncorroborated and sometimes anonymously sourced news reports—including, among others, the Rachel Maddow Show, Fox News, Wired Magazine, Bloomberg News, and Forbes. DHS commissioned its own National Cybersecurity and Communications Integration Center to produce a report for additional support. However, the resulting report lacks technical rigor and does not reflect specific knowledge (or a close examination) of how Plaintiffs' products actually operate. In its Final Decision, DHS

attempts to characterize the foregoing as "a substantial body of evidence"—but it comes nowhere close to meeting DHS's "substantial evidence" burden under the APA.

This is an important case for Kaspersky Lab, for the integrity of procedural due process, and for FISMA jurisprudence. Kaspersky Lab has spent decades and billions of dollars developing its reputation as a leading *defensive* cyber technology company, yet, without any advance notice, much less procedural protections or meaningful fact-finding, DHS labeled the Company's products "information security risks." At base, the BOD attempts to circumvent the D.C. Circuit's unequivocal requirement—set forth in a string of national security cases—that notice and a right to be heard *precede* government action effecting deprivation of a liberty interest. The BOD is also the government's first ever use of FISMA to achieve the permanent debarment of a major multinational company—circumventing well-established procedural protections under the Federal Acquisition Regulation. Perhaps most remarkable of all, DHS will argue that such an action is immune from judicial review.

The weight of authority, both with respect to fundamental procedural due process protections, as well as the courts' well-accepted role in reviewing agency fact-finding for discretionary abuses, rests heavily in favor of Kaspersky Lab. Accordingly, through this motion for summary judgment, Plaintiffs respectfully request the Court declare the BOD invalid and vacated, and remand to DHS with instructions to follow procedures that comport with due process and the APA.

STATEMENT OF FACTS

I. Background on Kaspersky Lab

Kaspersky Lab is a multinational cybersecurity company focused exclusively on protecting its customers against cyberthreats, no matter their origin. Declaration of Angelo

Gentile ("Gentile Declaration") ¶ 9. It is one of the world's largest privately owned cybersecurity companies, operating in 200 countries and territories and maintaining 35 offices in 31 countries. *Id*.

Plaintiff Kaspersky Lab, Inc. serves as the Company's North American headquarters, and is a Massachusetts corporation based in Woburn, Massachusetts. *Id*. at ¶ 4. It is a direct wholly-owned subsidiary of its U.K. parent, Plaintiff Kaspersky Labs Limited, the ultimate holding company for all Kaspersky Lab group entities. *Id*.

The Company's offices include research and development centers employing anti-malware experts in the U.S., Europe, Japan, Israel, China, Russia, and Latin America. *Id*. at ¶9. Over 400 million users—from governments to private individuals, commercial enterprise to critical infrastructure owners and operators alike—utilize Kaspersky Lab technologies to secure their data and systems. *Id*. Kaspersky Lab consistently ranks among the world's top four vendors of security solutions for endpoint users. *Id*.

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

The U.S. has been one of the most significant geographic markets in Kaspersky Lab's global business. *Id*. at ¶ 13. Sales to customers in the U.S. represented approximately one quarter of total global bookings in 2016. *Id*. A fraction of the Company's sales in the U.S. have been to the U.S. government, and have been driven by channel sales through independent

resellers. *Id*. at ¶ 15. Active licenses held by federal agencies at the time the BOD was issued had a total value to Plaintiffs of less than USD $54,000—approximately 0.03% of Plaintiff Kaspersky Lab, Inc.'s annual U.S. sales. *Id*. However, a much more significant part of the Company's business in the U.S. involve sales to current or potential federal government contractors who would now also be precluded by the BOD from purchasing and using Kaspersky Lab products in federal government information systems. *Id*. ¶¶ 23-25, 32. The value of that business is much more difficult to quantify. *Id*. ¶ 16.

II. DHS Published the BOD Without Affording Kaspersky Lab Notice or an Opportunity to Heard.

On July 18, 2017, well before the BOD was issued and without notice or prompting from DHS, Kaspersky Lab wrote to DHS. It did so in light of other U.S. government inquiries, offering to provide any information or assistance with regard to any investigation by DHS involving the Company, its operations, or its products, and without any knowledge of what, if any, action DHS was contemplating. AR 749-50 [Ex. A].[1] DHS responded on August 14, 2017, acknowledging the receipt of the Company's letter and its offer of assistance, and indicated that DHS "will be in touch again shortly." AR 940 [Ex. B]. DHS never was.

Rather, on September 13, 2017, DHS issued the BOD without affording any notice to Kaspersky Lab or a prior opportunity to rebut its allegations. AR 633-35 [Ex. C]. In the Decision memorandum accompanying the BOD, also dated September 13, 2017 ("Decision"), DHS explained that it issued the BOD pursuant to FISMA, which, as noted above, authorizes DHS to issue binding operational directives—"compulsory direction to agencies...for the purposes of safeguarding Federal information and information systems from a known or

[1] Pursuant to the Court's Scheduling and Procedures Order dated February 16, 2018 (Doc. 18), discrete portions of the Administrative Record cited herein are attached as Exhibits.

reasonably suspected information security threat, vulnerability, or risk." AR 628 [Ex. D] (*citing* 44 U.S.C.§ 3552(b)(1)). The Decision explained that DHS had "determined that the presence of Kaspersky-branded products…on federal information systems, presents a known or reasonably suspected information security threat, vulnerability, and risk to federal information and information systems…" *Id*. In addition, the Decision labeled Kaspersky Lab products a threat to U.S. national security based on the "ability of the Russian government, whether acting on its own or through Kaspersky, to capitalize on access to federal information and information systems provided by Kaspersky-branded products." AR 629 [Ex. D]. Specifically, the Decision claimed that "unclassified evidence" established that:

> As long as Kaspersky branded products are present on federal information systems, Kaspersky [Lab] or the Russian government will have the ability to exploit Kaspersky [Lab]'s access to those information systems for purposes contrary to U.S. national security, including viewing or exfiltrating sensitive data or installing malicious code on federal systems, such as through an update to the anti-virus software.

Id. The Decision also stated that DHS made "this determination based on the unclassified evidence alone," but adds that DHS also has "reviewed classified information that provides further support for this action." AR 631 [Ex. D].

The Decision cites a DHS Information Memorandum, dated September 1, 2017 (the "BOD Information"), authored by Jeanette Manfra ("Manfra") Assistant Secretary for Cybersecurity and Communications. The BOD Information was addressed to the then Acting DHS Secretary, through Christopher Krebs ("Krebs"), the Senior Official Performing the Duties of the Under Secretary. AR 3 [Ex. E]. DHS also issued a letter to Eugene Kaspersky dated September 13, 2017 (AR 637-38 [Ex. F]), and a press release that same day accompanying the BOD. Declaration of Ryan P. Fayhee ("Fayhee Decl."), ¶ 6, Ex. A.

The BOD compelled all federal agencies to:

(1) "Within 30 calendar days after issuance of [the BOD], identify the use or presence of Kaspersky-branded products on all federal informational systems and provide to DHS a report…";

(2) "Within 60 calendar days…develop and provide to DHS a detailed plan of action to remove and discontinue present and future use of all Kaspersky Lab-branded products beginning 90 day calendar days after issuance of [the BOD]"; and

(3) "At 90 calendar days...unless directed otherwise by DHS based on new information," begin actual removal, and provide a status report to DHS every 30 days until "full removal and discontinuance of use is achieved."

AR 634-35 [Ex. C]. ("30-60-90 day structure") The 30-day identification deadline fell on October 13, 2017, the 60-day removal plan deadline fell on November 12, 2017, and the 90-day deadline to begin removal fell on December 12, 2017.

III. The Purported Administrative Process

In issuing the BOD, DHS stated that it was providing an "administrative process to inform [DHS] decision making"—a process to be later set forth in a Federal Register Notice. AR 637 [Ex. F]. The BOD Decision and the letter by which it was conveyed to Plaintiffs contained only passing reference to the fact that an administrative process was to be provided to Plaintiffs and other affected parties. AR 628-32 [Ex. D]; AR 637 [Ex. F]. It was clear that a "process" was an afterthought and not a central part of the review and decision making process. *Id*.

Nearly a week later, on September 19, 2017, DHS announced in the Federal Register that it was permitting Plaintiffs (and any other affected parties) to initiate a review of the BOD by submitting to DHS "a written response and any additional information or evidence supporting the response, to explain the adverse consequences, address the Department's concerns, or mitigate those concerns." 82 Fed. Reg. 43,782, 43,784 (Fayhee Decl. Ex. B). DHS gave Plaintiffs until November 3, 2017 (subsequently extended to November 10, 2017), to respond to

the BOD. AR 746-47 [Ex. G]. The Federal Register further provided that, following DHS's receipt of a response to the BOD, "[T]he Secretary's decision will be communicated to the entity in writing by December 13, 2017." 82 Fed. Reg. 43,782, 43,784 (Fayhee Decl. Ex. B); AR 639-646 [Ex. H]. But December 13, 2017, was one day *after* the 90-day deadline by which agencies were to have begun removing Kaspersky Lab products. In an apparent acknowledgement of this procedural deficiency, the Information Memorandum accompanying the Final Decision "recommend[ed] that [the Acting Secretary] respond to Kaspersky and issue [her] Final Decision on or before Monday, December 11"—notwithstanding the December 13, 2017, deadline set forth in the Federal Register. *See* AR 754 [Ex. K], *infra*.

Defendants did not provide the BOD Information to Plaintiffs until September 29, 2017, (two weeks after the BOD had been issued, and Plaintiffs were notified), and then only following request of Plaintiffs' counsel. *See* Fayhee Decl. ¶ 5.

On November 10, 2017, Plaintiffs delivered to DHS the Kaspersky Lab Submission, an extensive written response to the BOD and its Information. AR 647-751 [Ex. I]. The Kaspersky Lab Submission rebutted at length the legal arguments and factual allegations levied against Plaintiffs, corrected many misunderstandings apparently held by DHS and perpetuated by the cited news reports, and highlighted the deficiencies in the administrative process offered by DHS. *See Id*.

Following the issuance of the BOD, DHS repeatedly declined the requests of Plaintiffs and their counsel to engage with them in order to present the Company's position, address DHS's concerns, and offer or discuss any potential options for mitigation. Fayhee Decl. ¶ 8.

Following the Kaspersky Lab Submission, DHS did agree to meet with Plaintiffs' representatives and counsel on November 29, 2017. *Id*. At that meeting, Plaintiffs responded to

a number of questions from DHS attorneys regarding the Kaspersky Lab Submission but DHS did not offer any further support for the BOD, much less an indication that it was willing to rectify any procedural or substantive deficiencies or consider any less draconian options short of the BOD's outright ban of Kaspersky Lab. *Id*. Plaintiffs believe that such options are available to DHS and were not fully explored either prior to or subsequent to the issuance of the BOD. *See* AR 647-83, AR 688-725 [Ex. I].

On December 6, 2017, DHS issued a "Final Decision maintaining BOD 17-01 without modification." (the "Final Decision"), AR 934 [Ex. J]. The Final Decision was accompanied by an Information Memorandum dated December 4, 2017, directed to the DHS Acting Secretary in support of the Final Decision (the "Final Information") (AR 752-76 [Ex. K]) (and Exhibits 1-10)[2], and a Letter to Eugene Kaspersky. AR 938 [Ex. L].

Among other evidence and arguments never before disclosed by DHS, the Final Decision and the Final Information introduced for the first time "an analysis of relevant portions of Russian law prepared by Professor Peter Maggs of the University of Illinois College of Law (the 'Maggs Report')." *See* AR 752 [Ex. K] and AR 777-821 [Ex. M]. Rather than introducing the Maggs Report with the September 13, 2017, BOD, which would have enabled Plaintiffs to address and/or rebut the report when Plaintiffs filed the Kaspersky Lab Submission, DHS did not share the report until its December 6, 2017, Final Decision. *See* AR 935 [Ex. J]. This foreclosed any opportunity for Plaintiffs to rebut or contest the Maggs Report, and other materials introduced at the time of the Final Decision.

[2] Those exhibits (spanning AR 777-933) are not attached hereto, except for the Peter Maggs Report as discussed herein.

IV. The Immediate Effect of the Debarment

Although the BOD's 30-60-90 day structure gives the impression that harm is not immediate, the BOD effected an immediate and complete debarment of Kaspersky Lab from government business upon issuance. At a November 14, 2017, Hearing of the Committee on Science, Space, and Technology of the U.S. House of Representatives ("Bolstering the Government's Cybersecurity: A Survey of Compliance with the DHS Directive"), Manfra testified that some agencies had *already* proceeded with removal of Kaspersky products without regard to the 30-60-90 day structure:

> "We're working with each agency individually…[S]ome of them have chosen to go ahead and remove the products ahead of schedule…Not all of the Agencies have submitted the required action plan as I mentioned…[S]ome of them have gone ahead and just identified a way to remove the software so they are going about that."[3]

This testimony was made just four days after Plaintiffs submitted the Kaspersky Lab Submission to DHS, and Manfra testified that she had not yet even had an opportunity to review Plaintiff's response.[4] Thus, federal agencies had begun removing Kaspersky Lab software long before DHS even had completed its review of the Kaspersky Lab Submission. Likewise, in statements made to the media following the Final Decision, Krebs (as noted above, DHS Senior Official Performing the Duties of the Under Secretary) confirmed that with his oversight, federal agencies had actually been removing Kaspersky Lab-branded software prior to the 90-day mark. Fayhee Decl. Ex. C at p. 2 ("For the most part, we're closed out on removing the Kaspersky [antivirus]-branded products")(alternation in original).

---

[3] *Bolstering the Government's Cybersecurity: A Survey of Compliance with the DHS Directive*, 115th Cong. (2017), at 55:32 (statement of Jeanette Manfra, DHS), *available at* CQ Transcription of Nov. 14, 2017 House Subcommittee on Oversight Hearing - Bolstering the Government's Cybersecurity: A Survey of Compliance with the DHS Directive, p. 11. Fayhee Decl. Ex. D.

[4] *Id*. at 10.

Amazon.com customer reviews also clearly show that the BOD prejudiced commercial and consumer opinions as soon as it was issued in September 2017. *See* Fayhee Ex. E. None of these reviews from September through November 2017 reflect customers waiting for DHS's "Final" decision to come in December 2017. *Id.* For example, one customer writes this review about Kaspersky Lab's products:

> **As of September, banned by the US from use in all federal agencies and departments**
> Have removed from all my computers and cleaned my registry. *As of last month (Sept 2017)*, the US gov't has banned the use of this software by all federal agencies and departments, due to its suspected (or proven, depending on who you believe) links to the Russian government. Do a google search for 'Kaspersky DHS' to see for yourself…Internet Security programs have access to every file on your computer, which they can send wherever they want. *Strongly suggest uninstalling and buying something else!*

Id. at p. 1 (emphasis added).[5] The BOD covers the same products used by commercial customers and individual customers, and has had a significant adverse effect on the reputational interest of the Company as evidenced by the perceptions of current and potential users. Gentile Decl. at ¶ 18.

DHS intended the BOD to have precisely this impact. In his public statements on October 31, 2017, Krebs was blunt about DHS's intent: "[W]hen [DHS] makes a pretty bold statement like issuing the Kaspersky binding operational directive I think that's a fairly strong signal [to consumers]."[6]

The reputational damage had an immediate and severe financial impact on Kaspersky Lab—specifically on its U.S. commercial and consumer sales—and this impact is continuing and

---

[5] Amazon shows a February 12, 2017, date in connection with this review, but the review was written in October 2017. *See Id.* As noted, the review states: "*As of last month (Sept 2017)*…" *Id.* (emphasis added).

[6] *See* Aspen Institute, *Is the US Losing the Cyber Battle?*, at 57:56, October 31, 2017, https://www.aspeninstitute.org/events/us-losing-cyber-battle/.

growing. Gentile Decl. at ¶¶ 18-24. Several U.S. retailers removed Kaspersky Lab products from their shelves and suspended their long-standing partnerships with Kaspersky Lab following the issuance of the BOD. *Id*. at ¶ 26. Some of these retailers, which previously provided a steady stream of both new customers and consumer product subscription renewals to Kaspersky Lab over the years, went even further. *Id*. Upon removing Kaspersky Lab products from their shelves and online offerings, these retailers encouraged and otherwise incentivized existing Kaspersky Lab software customers (current license holders) to "switch" to one of the Company's competitors. *Id*. Kaspersky Lab, Inc.'s 2017 Q3 gross bookings from retail sales in the U.S. fell 37% compared to the same period in 2016. *Id*. And, the Company's gross bookings from U.S. retail sales in 2017 Q4 fell 61% compared to the same period in 2016. *Id*. at ¶ 27. Overall, Kaspersky Lab, Inc.'s gross bookings from U.S. retail sales in the second half of 2017 fell 50% compared to the same period in 2016. *Id*.

In addition to the decline in the consumer market, Kaspersky Lab, Inc.'s business-to-business ("B2B") sales have also been negatively impacted since the issuance of the BOD. *Id*. at ¶ 30. Kaspersky Lab, Inc.'s 2017 bookings from B2B sales fell 33% in Q3 and 45% in Q4 when compared to the same period in 2016. *Id*. at ¶ 31. The B2B renewal rate has gone down 36 percentage points to only 26% of existing corporate customers renewing in January 2018 from 62% of such customers renewing in the same period last year. *Id*.

Further, several substantial tenders for the provision of Kaspersky Lab products in process at the time of the BOD were terminated by customers as a result of its issuance, in many cases before the Final Decision was issued. *Id*. at ¶ 19. The potential B2B customers often reiterated their belief that Kaspersky Lab is the best technical solution for their needs, but that they were unwilling or unable to proceed with the purchase due to the DHS action. *Id*.

Even where its partners have recently been successful in making sales of Kaspersky Lab products, the Company is receiving and processing an unprecedented volume of product return and early termination requests. *Id*. at ¶ 20. Many customers returning the software for a refund specifically cite the BOD, and these concerns are difficult to address so long as the BOD remains in effect. *Id*. Net loss from product returns to Kaspersky Lab, Inc. from U.S. customers from September through December 2017 totalled $237,312.73. *Id*. at ¶ 29. By contrast, net loss from product returns during the same period last year totalled $10,033.16. *Id*. Kaspersky Lab's position as a trusted software vendor has been compromised in all areas, which has resulted in the Company accepting returns that would otherwise have been rejected under its standard return policy. *Id*. at ¶ 20.

The BOD immediately caused further collateral harm to Kaspersky Lab by inducing a number of States to follow suit in issuing directives prohibiting their own State and local agencies from using Kaspersky Lab products, and mandating their removal (the "State Directives"). *Id*. at ¶ 38. Some of these State Directives are specifically based on, and exclusively refer to, the BOD as their justification, and did not wait for the expiration of the 90-day period or the issuance of DHS's Final decision, before making their own determinations. *Id*. Rather, they simply repeat the language DHS used in support of the BOD, absent any further validation. *Id*.

The first instance of such a State Directive that specifically refers to the BOD appeared in New York State, only two days after the BOD. *Id*. at ¶ 39. On September 15, 2017, the New York Office of General Services issued General Information Bulletin CL # 843[7] (the "New York Directive"), the purpose of which is to "advise authorized users of centralized information

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

technology contracts established by the New York State Office of General Services ("OGS") of data privacy and security concerns related to products sold by Kaspersky Lab." *Id*. The next sentence reads "On September 13, 2017, the U.S. Department of Homeland Security ("DHS") directed federal agencies to identify, remove, and discontinue current and future use of products manufactured by Kaspersky Lab, a Russian cybersecurity and software company that DHS characterized as possibly vulnerable to Russian government influence..." *Id*. The New York Directive concludes with recommendations that New York State departments to contact their IT departments "to commence a review of purchases and contracts for software and services to determine their exposure to Kaspersky Lab products and services." *Id*.

The second instance of such State Directives that specifically refer to the BOD appeared in Texas. On October 30, 2017, the Texas Education Agency issued a Cyber Alert titled "DHS Issues Binding Operational Directive on Kaspersky Products"[8] (the "Texas Directive"), which contains a summary of the BOD and follows with two recommendations. *Id*. at ¶ 40. The Texas Directive concludes by recommending that, in light of the high volume of sensitive student information collected, Education Service Centers and Local Educational Agencies in Texas "follow the guidance in the federal directive." *Id*. Immediately following the Texas Directive, several existing customers from the education sector in Texas informed Kaspersky Lab's reseller partner that the Education Service Centers were immediately directing school boards to remove Kaspersky Lab software from their machines and networks. *Id*. As a result, affected customers demanded refunds for the Kaspersky Lab software subscriptions they were prohibited from using. *Id*.

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

V. Kaspersky Lab's Challenge to the National Defense Authorization Act for FY 2018

On December 12, 2017, President Trump signed into law the National Defense Authorization Act for FY 2018, Pub. Law No. 115-91, § 1634 ("NDAA"), which includes Section 1634 ("Prohibition on Use of Products and Services Developed or Provided by Kaspersky Lab"). That statute, which takes effect on October 1, 2018, prohibits the entire federal government from using any product or service that comes directly or indirectly from Kaspersky Lab: "No department, agency, organization, or other element of the Federal Government may use...any *hardware, software, or services* developed or provided, *in whole or in part*, by…Kaspersky Lab…" *Id*. § 1634 (a) and (b)(emphasis added).[9] Importantly, this statute bans the government's use of any third-party hardware or software which embeds any computer code from Kaspersky Lab.

Unlike the BOD, which labels Kaspersky Lab products an "information security risk," the NDAA on its face does not explicitly offer any justification for the ban. *See* Fayhee Decl. Ex. A; Pub. Law No. 115-91 § 1634. The NDAA's legislative history is equally devoid of any fact-finding or floor debate concerning the ban. The only commentary surrounding the NDAA ban comes from extra-legislative statements (*i.e.*, press releases, and newspaper opinion pieces) of Senator Jeanne Shaheen, who introduced the amendment to the NDAA effecting the ban.[10]

[9] The BOD ban, by contrast, is limited to software, excludes "Kaspersky Threat Intelligence and Kaspersky Security Training," and "does not address Kaspersky code embedded in the products of other companies." AR 634 [Ex. C]. The BOD also expressly excepts from its scope National Security systems. AR 633 [*Id*.].

[10] The legislative history of NDAA § 1634 is set forth in the Complaint filed in *Kaspersky Lab, Inc., et al. v. United States*, 18-cv-00325-CKK (D.D.C.). *See* ¶¶ 24-37 (and exhibits) therein.

Section 1634(b) expressly provides that that the "Effective Date" for this ban is October 1, 2018, and DHS has expressly acknowledged that the BOD is currently the "operative prohibition" against Kaspersky Lab:

> Unlike the statutory provision, BOD 17-01's direction to remove Kaspersky-branded products from federal information systems is effective on December 12, 2017, unless DHS directs otherwise. As stated above, the NDAA prohibition is not effective until October 2018. Thus, until October 1, 2018, the BOD's requirement to start removal on Day 90, unless modified or rescinded by you, *is the operative prohibition on agency use of Kaspersky products*.

AR 756-57 [Ex. K]. (emphasis added).

On February 12, 2018, Kaspersky Lab filed a lawsuit in this Court to invalidate Sections 1634(a) and (b) as an unconstitutional bill of attainder, on the grounds that they single out Kaspersky Lab for punishment without a judicial trial. *See* Complaint, *Kaspersky Lab, Inc., et al. v. United States*, 18-cv-00325-CKK (D.D.C.).

STANDING

To establish Article III standing, a "plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016), *citing Lujan v. Defenders of Wildlife,* 504 U.S. 555, 560-61 (1992). The injury for standing "need not be significant; an identifiable trifle will suffice." *Southern Mut. Help Ass'n, Inc. v. Califano*, 574 F.2d 518, 523 (D.C. Cir. 1977), *citing United States v. Students Challenging Regulatory Agency Procedures* (SCRAP), 412 U.S. 669, 689 n.14 (1973). Here, Plaintiffs have standing based on both (i) reputational injury caused by the BOD, which in turn is causing substantial financial injury to the Company, and (ii) the loss of the legal right to the U.S. government.

I. The BOD has Caused Profound Reputational Injury to Plaintiffs.

It is beyond dispute that the BOD is causing and will continue to cause profound reputational harm to Kaspersky Lab. Accompanying the issuance of the BOD, DHS issued a press release on September 13, 2017, announcing that the BOD "is based on the *information security risks* presented by the use of Kaspersky products on federal information systems":

> Kaspersky anti-virus products and solutions provide broad access to files and elevated privileges on the computers on which the software is installed, *which can be exploited by malicious cyber actors to compromise those information systems*…The risk that the Russian government, whether acting on its own or in collaboration with Kaspersky, could capitalize on access provided by Kaspersky products to c*ompromise federal information and information systems* directly implicates U.S. national security…The Department's priority is to ensure the integrity and security of federal information systems. Safeguarding federal government systems r*equires reducing potential vulnerabilities, protecting against cyber intrusions, and anticipating future threats*.

Fayhee Decl. Ex. A at 1-2. (emphasis added). About a week later, on September 19, 2017, DHS published the BOD in the Federal Register. (DHS "has determined that the risks presented by Kaspersky-branded products justify issuance of this [BOD].") 82 Fed. Reg. 43,782, 43,783 (Sept. 19, 2017) (*Id*. Ex. B).

Kaspersky Lab markets itself as a leading *defensive* cyber technology company, focused exclusively on *protecting against* cyber threats no matter their origin, and so, in labeling the Plaintiffs' products as a cyber threat, the BOD caused immediate harm to the Company's reputation. Gentile Decl. at ¶ 17-24. The reputational harm was realized as soon as the BOD was issued, as illustrated by way of example, on Amazon.com customer reviews. Fayhee Decl. Ex. E. In fact, one of the Amazon customer reviews referenced above copied and pasted portions verbatim from the DHS press release. *Id*. at p. 2 (see review by "Aircarl on September 13, 2017").

The Company has standing based on reputational injury, both now, while the BOD is the "operative prohibition" against the Company[11]—and after October 2018, when the NDAA becomes effective, as the Company's reputation will continue to suffer directly from the explicit "information security threat" label. As the D.C. Circuit held in *Foretich v. United States*, 351 F.3d 1198, 1213 (D.C. Cir. 2003), "where reputational injury derives directly from an unexpired and unretracted government action, that injury satisfies the requirements of Article III standing to challenge that action."

Indeed, *Foretich* is particularly instructive here, as the D.C. Circuit held the plaintiff had standing to challenge an otherwise moot federal law because of its direct reputational injury. *Id*. at 1211-1216. The plaintiff, Dr. Foretich, was accused by his ex-wife of sexually molesting their daughter, and his reputation was thereafter sullied by the media and certain lawmakers. *Id*. at 1203-04. Congress enacted the Elizabeth Morgan Act, which, while not expressly specifying Dr. Foretich by name, singularly applied to him as a means to restrict his child visitation rights. *Id*. at 1204. The D.C. Circuit held that because of the direct reputational injury, Dr. Foretich had standing to challenge the Act as an unconstitutional bill of attainder, even though the Act no longer had any legal effect, given that his daughter had since become an adult. *Id*. at 1212-16.

[11] *See generally, Southern Mut. Help Ass'n, Inc. v. Califano*, 574 F. 2d 518, 524 (D.C. Cir. 1977)("[The injury] that is capable of direct redress by this court…and clearly traceable to the action by [the government], is the assertion by [plaintiff] that its good name and reputation have been damaged. For an organization such as [plaintiff], dependent as it is upon grants for its very existence, a good reputation is perhaps its most valuable asset."); *Rangel v. Boehner*, 20 F. Supp. 3d 148, 160 (D.D.C. 2013) (holding that Congressman's censure was injury-in-fact to his reputation: "[I]t is beyond peradventure that being censured by the U.S. House of Representatives concretely and particularly harms a sitting Member's reputation, particularly a Member like Rangel who has demonstrated a desire to remain in the House."); *ACORN v. United States*, 618 F.3d 125, 134 (2d Cir. 2010)(plaintiffs had standing because even "if [they] are not and never will be interested in applying for grants or funding from the Department of Defense, the fact that the Defense Department's appropriations law specifically prohibits [them] from being eligible for federal funds affects [their] reputation with other agencies, states, and private donors.")

This is because the Act "directly damages his reputation and standing in the community by effectively branding him a child abuser and an unfit parent." *Id*. at 1214. The D.C. Circuit observed that [o]nce a prominent oral surgeon, Dr. Foretich's business suffered a 30% decline following adoption of the Act," and he was "[f]orced to seek employment outside of northern Virginia, [and] denied a position at a North Carolina university in part because of the Act." *Id*. at 1209. Most notably, the D.C. Circuit rejected the government's arguments that other sources of reputational harm—the custody and other legal proceedings, which "gained extraordinary notoriety in the media"—inhibited traceability or redressability with respect to his reputational injury based on the otherwise moot Act:

> It may be true, as the Government argues, that the damage to Dr. Foretich's reputation comes in part from the publicity surrounding the custody dispute and…not solely from the Elizabeth Morgan Act. But this misses the point. The Act itself has caused significant harm to Dr. Foretich. Therefore, by vindicating Dr. Foretich's assertion that Congress unfairly and unlawfully rendered a judgment as to his character and fitness as a father, declaratory relief will provide a significant measure of redress sufficient to satisfy the requirements of Article III standing. Here, a decision declaring the Act unlawful would make clear that Congress was wrong to pass judgment on Dr. Foretich and wrong to single him out for punishment on the basis of that judgment. In doing so, a declaratory judgment in Dr. Foretich's favor would give redress for his reputational injuries.

See Id. at 1203, 1216.

The same is true regarding the BOD after the NDAA becomes effective in October 2018. The reputational harm is not a mere "byproduct" of the BOD, and will not be a "lingering effect of an otherwise moot government action" in October 2018. *See Id*. at 1212. Nor will the Company's reputational injury be "'a secondary effect of an otherwise moot action.'" *Id*., *quoting Penthouse Int'l, Ltd. v. Meese*, 939 F.2d 1011, 1019 (D.C. Cir. 1991). Rather, the reputational harm will be the primary and continuing effect of an unrevoked order. The BOD alone labels Kaspersky Lab an "information security risk"—and it does so on the explicit

grounds that the Company's products "can be exploited by malicious cyber actors to compromise…information systems." Fayhee Decl. Ex. A.

Plaintiffs have submitted evidence of customers (both retail and commercial) specifically citing the BOD (rather than any other source) as the reason they decided not to make a purchase—or decided to return—Plaintiffs' products. *See* Fayhee Decl., Ex. E; Gentile Decl. ¶¶ 19-24, 32-36, 42. Just as Dr. Foretich established redress without showing that his former patients who had left his practice would return upon invalidation of the Act, or demonstrating that other specific reputation-based harms to his career had been undone, Kaspersky Lab may establish this element without showing its lost customers would actually re-engage its products upon rescission of the BOD. *See Foretich*, 351 F.3d at 1214, 1216.

In sum and substance, the BOD's reputational injury does now and will continue to provide a basis for standing so long as the BOD remains unrescinded, notwithstanding other sources of reputational harm.

II. Plaintiffs are also Injured by their Loss of Legal Right to Sell to the Government.

The Company also has standing based on the deprivation of the legal right to sell to the U.S. government. As former Chief Justice Burger explained, contractors doing business with the government "have a right not to be debarred except in an authorized and procedurally fair manner…" *Gonzalez*, 334 F.2d at 576 (holding that "[plaintiff's] allegations of the means by which debarment was imposed in this case set forth a claim of invasion of that right and give them standing under [the APA].") Rescission of the BOD would restore the loss of this legal right. That the government may or may not chose to actually purchase from the Company (should the BOD be rescinded) is beside the point. *See, e.g., Idaho Bldg. & Const. Trades*

Council v. Wasden, 32 F. Supp. 3d 1143 (D. Id. 2014), *citing FEC v. Akins*, 524 U.S. 11, 25 (1998)(rejecting government's argument that invalidation of law banning project labor agreements would fail to provide redress as government would never consider using project labor agreement in a public works project anyway.)

Nor does the NDAA foreclose redress to this injury. As this Court has held, "[a] claim is justiciable 'so long as the relief sought would constitute a necessary first step on a path that could ultimately lead to relief fully redressing the injury.'" *American Petroleum Tankers Parent, LLC v. United States,* 943 F. Supp. 2d 59, 66 (D.D.C. 2013)(J. Kollar-Kotelly), *quoting Tel. & Data Sys., Inc. v. FCC*, 19 F.3d 42, 47 (D.C. Cir. 1994)("plaintiff may not ultimately prevail if the Court vacates the Administrator's decision, but it cannot prevail unless the Court does so, which is sufficient to satisfy the redressability requirement for constitutional standing.")(internal quotation and alterations omitted). Put differently, "[Plaintiffs] do not have to surmount every obstacle simultaneously…and [are] entitled to tackle one roadblock at a time." *Idaho Bldg.*, 32 F. Supp. 3d at 1153, *quoting Ibrahim v. DHS*, 669 F.3d 983, 993 (9th Cir. 2012). With reliance on this rule, the court in *Idaho Building* specifically rejected the government's argument that the subsequent enactment of a "nearly identical statute" to the one challenged foreclosed redressability, and held that plaintiffs had standing to continue their challenge against the earlier enacted statute. *Id*. at 1147, 1153.

The same is true here and the Plaintiffs *have* in fact challenged the NDAA, putting them on an even stronger footing.

III. Standing Requirements Applicable to Kaspersky Labs Limited

Kaspersky Labs Limited, the U.K. parent,[12] has standing to assert a violation of Fifth Amendment due process, which is the basis for its second APA claim. "[A]liens receive constitutional protections when they have come within the territory of the United States and developed substantial connections with this country." *United States v. Verdugo-Urquidez*, 494 U.S. 259, 271 (1990). In *National Council of Resistance of Iran v. Dep't of State*, 251 F.3d 192, 200-202 (D.C. Cir. 2001), for example, the D.C. Circuit observed that a designated terrorist organization was entitled to Fifth Amendment due process protections because of its "substantial connections with this country" observing the organization "has an overt presence within the National Press Building in Washington, D.C." and "claims an interest in a small bank account." (internal quotations omitted).

Kaspersky Labs Limited clearly has "substantial connections" to the U.S. that afford it due process protections. *Verdugo-Urquidez*, 494 U.S. at 271. As explained above, Kaspersky Labs Limited's wholly-owned subsidiary, Kaspersky Lab, Inc., serves as the North American headquarters through offices in Woburn, Massachusetts, and employed close to 300 people just before issuance of the BOD. Gentile Decl. ¶¶ 4, 43. Sales to customers in the U.S. represented approximately one quarter of total Kaspersky Lab global bookings in 2016, and one fifth of total global bookings in 2017. *Id*. at ¶ 41. And, the Massachusetts subsidiary has invested over half a billion dollars in the U.S. over the last thirteen years, and over $60 million in 2017 alone. *Id*. at ¶

[12] In addition to the reputational injury and loss of opportunity to sell to the U.S. Government, the U.K. parent also has Article III standing because the BOD "cause[s] [Kaspersky Labs Limited] actual financial injury…by…reducing the return on [its] investment in [Kaspersky Lab, Inc.] and by lowering the value of [its] stockholdings in [that subsidiary]." *See Franchise Tax Bd. v. Alcan Aluminum Ltd*., 493 U.S. 331, 336 (1990). Indeed, although sales to customers in the U.S. represented approximately one quarter of total global bookings in 2016, the U.S. accounted for only one fifth of total global bookings in 2017. Gentile Decl. ¶ 41.

14. These are clearly "substantial connections" to this country, and support Kaspersky Labs Limited's standing to assert a violation of constitutional due process.

LEGAL STANDARD FOR SUMMARY JUDGMENT

"[W]hen a party seeks review of agency action under the APA, the district judge sits as an appellate tribunal. The entire case on review is a question of law." *Am. Coll. of Emergency Physicians v. Price*, 264 F. Supp. 3d 89, 93 (D.D.C. 2017)(J. Kollar-Kotelly), *quoting Am. Bioscience, Inc. v. Thompson*, 269 F.3d 1077, 1083 (D.C. Cir. 2001)(alteration omitted). "Summary judgment is [ ] the mechanism for deciding whether as a matter of law the agency action is supported by the administrative record and is otherwise consistent with the APA standard of review." *Id*., *quoting Southeast Conference v. Vilsack*, 684 F. Supp. 2d 135, 142 (D.D.C. 2010).

"The APA…provides that a reviewing court shall 'hold unlawful and set aside agency action' that is 'not in accordance with law' or 'contrary to constitutional right.'" *Poett v. United States*, 657 F. Supp. 2d 230, 241 (D.D.C. 2009)(J. Kollar-Kotelly); 5 U.S.C. §§ 706(2)(A) & (B). "In contrast to the deferential standard of review [for non-constitutional APA claims], a court's review of 'constitutional challenges to agency actions…is *de novo*.'" *Id., quoting, Cullman Reg'l Med. Ctr. v. Shalala*, 945 F. Supp. 287, 293 (D.D.C. 1996). *See also, Id*. ("[R]eview of constitutional claims under the APA mirrors review under the Constitution itself")(internal quotation omitted).

With respect to Plaintiffs' non-constitutional claim, to survive the "arbitrary and capricious" standard, the agency is required to "examine the relevant data and articulate a satisfactory explanation for its action including a rational connection between the facts found and the choice made." *Am. Coll. of Emergency Physicians*, 264 F. Supp. 3d at 93-94, *quoting Motor*

Vehicle Mfrs. Ass'n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co., 463 U.S. 29, 43. "Moreover, an agency cannot 'fail to consider an important aspect of the problem' or 'offer an explanation for its decision that runs counter to the evidence' before it.'" *Id., quoting Dist. Hosp. Partners, L.P. v. Burwell*, 786 F.3d 46, 57 (D.C. Cir. 2015)(alterations omitted).

Finally, "the arbitrary and capricious test…subsum[es] the substantial evidence test…" *Larkin Chase Nursing & Restorative Ctr. v. Shalala*, 2001 U.S. Dist. LEXIS 23655, *16 (D.D.C. Feb. 6, 2001)(internal quotations omitted); *see generally*, *Ass'n of Data Processing v. Bd. of Governors*, 745 F. 2d 677, 683-84 (D.C. Cir. 1983)("When the arbitrary or capricious standard is performing that function of assuring factual support, there is no *substantive* difference between what it requires and what would be required by the substantial evidence test, since it is impossible to conceive of a 'nonarbitrary' factual judgment supported only by evidence that is not substantial in the APA sense...")(emphasis in original)

ARGUMENT

I. The BOD Violated Plaintiffs' Fifth Amendment Due Process Rights.

Plaintiffs' first claim is that the BOD violates their Fifth Amendment due process rights. As explained above, the Court "owes no deference to the agency's pronouncement on [this] constitutional question, and must instead make an independent assessment of [Plaintiffs'] claim of constitutional right when reviewing [the] agency decision-making." *Poett*, 657 F. Supp. at 241, *quoting Lead Indus. Ass'n v. EPA,* 647 F.2d 1130, 1173-74 (D.C. Cir. 1980).

"To state a claim for the denial of procedural due process, a plaintiff must allege that (1) the government deprived [the plaintiff] of a liberty or property interest to which [the plaintiff] had a legitimate claim of entitlement, and (2) that the procedures attendant upon that deprivation were constitutionally [in]sufficient." *Jefferson v. Harris*, 170 F. Supp. 3d 194, 204 (D.D.C. 2016)

(internal quotations omitted). Here, DHS deprived the Company of a liberty interest by debarring it and impugning its reputation, and effected this deprivation without any prior notice or opportunity to be heard.

A. The BOD deprived Kaspersky Lab of a Liberty Interest.

"[A] person's right to... follow a chosen profession free from unreasonable governmental interference comes within the 'liberty'...concept of the Fifth Amendment," and "this 'liberty concept' protects corporations as well as individuals." *Trifax Corp. v. District of Columbia*, 314 F. 3d 641, 643 (D.C. Cir. 2003)(internal quotations omitted). The BOD deprived Kaspersky Lab of this liberty interest by (1) effecting a formal debarment of the Company from selling to the U.S. government, and removing previously installed software, (2) impugning Kaspersky Lab's reputation in the process of that debarment (under the so-called "reputation-plus" theory), and (3) stigmatizing it in that process (under the so-called "stigma-plus" theory).

First, "formally debarring a corporation from government contract bidding constitutes a deprivation of liberty that triggers the procedural guarantees of the Due Process Clause." *Id*. ("Had the District formally debarred Trifax from bidding on government contracts, that would have unquestionably constituted a deprivation of liberty.") *See also, Abdelfattah v. Dep't of Homeland Sec*., 787 F.3d 524, 538 (D.C. Cir. 2015)("[W]hen the government formally debars an individual from certain work or implements broadly preclusive criteria that prevent pursuit of a chosen career, there is a cognizable deprivation of liberty that triggers the procedural guarantees of the Due Process Clause.")(quotation omitted); *BMY, Div. of HARSCO Corp. v. United States*, 693 F. Supp. 1232, 1241 (D.D.C. 1988)("A suspension or debarment, be it formal or constructive, is legal only if the contractor has been afforded full due process protections.")(citations omitted).

The BOD unquestionably effected a formal debarment. The BOD expressly orders all federal agencies to indefinitely "discontinue…future use of all Kaspersky-branded products" as well as to remove previously installed Kaspersky Lab products. AR 634 [Ex. C]. In fact, DHS's Decision contains an entire section entitled "**DEBARMENT**." AR 631 [Ex. D]. Therein, DHS explains that the BOD "is a more appropriate process than a debarment proceeding" under the Federal Acquisition Regulation ("FAR")—principally because the BOD is more extensive and severe: the BOD is not only prospective, but also retrospective (reaching previously purchased products), requires the removal of Kaspersky Lab-branded products "indefinitely," and prevents third parties from selling products produced by Kaspersky Lab. *Id*.

Second, "under the reputation-plus test[,] a protected liberty interest may be implicated if the Government effectively bars a contractor from virtually all Government work due to charges that the contractor lacks honesty or integrity." *New Vision Photography Program, Inc. v. District of Columbia*, 54 F. Supp. 3d 12, 31 (D.D.C. 2014)(internal quotation omitted). This is because "[w]here a person's good name, reputation, honor, or integrity is at stake because of what the government is doing to him, that person's liberty interest is on the line, meaning that notice and an opportunity to be heard are essential." *Liff v. Office of Inspector Gen. for the U.S. Dep't of Labor*, 156 F. Supp. 3d 1, 10 (D.D.C. 2016)(internal quotations omitted).

Here, DHS labeled Kaspersky Lab's anti-virus products "information security risks" and summarily ordered their identification, removal, and discontinuation by all subject U.S. government agencies. Fayhee Decl. Ex. A; AR 633-35 [Ex. C]. On the strength of media reports nearly alone, DHS's press release accompanying the BOD essentially alleges that Kaspersky Lab is an arm of Russian intelligence services:

> [DHS] is concerned about the ties between certain Kaspersky officials and Russian intelligence and other government agencies, and requirements under Russian law that allow Russian intelligence agencies to request or compel assistance from

> Kaspersky and to intercept communications transiting Russian networks. The risk that the Russian government, whether acting on its own or in collaboration with Kaspersky, could capitalize on access provided by Kaspersky products to compromise federal information and information systems directly implicates U.S. national security.

Fayhee Decl. Ex. A at 1. These statements unquestionably impugn Kaspersky's Lab's reputation and integrity. Based on these stated concerns, Kaspersky Lab is "effectively barr[ed] from virtually all Government work." *See New Vision Photography,* 54 F. Supp. 3d at 31 (internal quotation omitted).

Third, a "stigma-plus" claim "arises when the government imposes a stigma or other disability that forecloses the plaintiff's freedom to take advantage of other employment opportunities." *Liff v. Office of the Inspector Gen. for the U.S. Dep't of Labor,* 2016 U.S. Dist. LEXIS 153979, *21, *22 (D.D.C. Nov. 7, 2016)(explaining that relative to its "reputation-plus counterpart...the types of official actions that are recognized are somewhat broader in the stigma-plus context," and "in stigma-plus cases, official speech is not necessarily implicated.") Under this theory, "a plaintiff may show that (1) the [government] action formally or automatically exclude[d] [her] from work on some category of future [government] contracts or from other government employment opportunities or (2) that the [government] action does not have this binding effect, but nevertheless has the broad effect of largely precluding [her] from pursuing her chosen career." *Id*. at *22. (internal quotations omitted)(emphasis in original).

The BOD does the former—it "formally or automatically exclude[s] [Kaspersky Lab] from bidding for government contracts." *See Trifax Corp. v. District of Columbia* 2001 U.S. Dist. LEXIS 27208, at *16 (D.D.C. Nov. 1, 2001). *See also generally, Kartseva v. Dep't of State*, 37 F.3d 1524, 1528 (D.C. Cir. 1994)(holding that firing of a government contractor working as Russian translator—based on "counterintelligence concerns"—would implicate a liberty interest

if the State Department's action "formally or automatically excludes [the plaintiff] from work on some category of future State contracts or from other government employment opportunities").

Under any and all of these articulated theories, the BOD deprived Kaspersky Lab of liberty interests, and this element is therefore met.

B. The BOD's Procedures were Constitutionally Insufficient.

1. Pre-deprivation Process was Required Under the *Mathews v. Eldridge* Test.

In depriving Kaspersky Lab of a protected liberty interest, the BOD violated Kaspersky Lab's Fifth Amendment rights because the BOD afforded no pre-deprivation process. Although due process is flexible and calls for such procedural protections as the particular situation demands, "[d]ue process *ordinarily* requires that procedures provide notice of the *proposed* official action and the opportunity to be heard at meaningful time and in a meaningful manner." *Ralls Corp. v. Comm. on Foreign Inv. in the U.S.*, 758 F.3d 296, 318 (D.C. Cir. 2014)(internal quotations omitted)(emphasis added). Specifically, DHS should have provided pre-deprivation notice and an opportunity to be heard pursuant to the three-factor test set forth in *Mathews v. Eldridge*, 424 U.S. 319, 335 (1976). *Mathews* held that "identification of the specific dictates of due process generally requires consideration of three distinct 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 function involved and the fiscal and administrative burdens that the additional or substitute procedural requirement would entail.

Id. As explained below, each of these three factors—and all of them combined—weigh heavily in favor of required pre-deprivation process here.

a. Kaspersky Lab Has a Substantial Private Interest in its Ability to Sell to the Government and in its Reputation.

It is beyond dispute that Kaspersky Lab has a substantial private interest in its ability to sell its software products to federal agencies, and in its reputation as a market-leading anti-virus software developer. *See* Gentile Decl. ¶¶ 18, 24. It makes little difference that, quantitatively, Kaspersky Lab's sales, through its partners, to the U.S. government historically have been a fraction of the company's total sales. *Id*. at ¶¶ 15, 18. Clearly, DHS's labeling of Kaspersky Lab's antivirus software products as "information security risks," its other inflammatory remarks, and its summarily banning the Company from all government agencies has had a profound qualitative impact on the Company's brand, reputation, and prospects everywhere it does business. *Id*. at ¶ 18. Indeed, such harm was DHS's specific intent, as detailed above.

b. DHS's Process Entailed a High Risk of Erroneous Deprivation, and Additional or Substitute Procedural Safeguards Would Have Been Valuable.

With respect to the high risk of erroneous deprivation in the second *Mathews* factor, it bears repeating: DHS has publicly stated that it has *no conclusive evidence* that Kaspersky Lab had facilitated the breach of any U.S. government information system.[13] The risk is compounded by the highly technical nature of the subject matter and compounded yet further by DHS's reliance on media reports rather than on its own fact-finding. The preordained outcome also heightens this risk: as noted above, the Final Decision originally was due after the 90-day mark. DHS went so far as to expressly acknowledged that many agencies disregarded the 30-60-90 day structure, and began removal of the software before day 90. *See* Facts (Section IV), *supra*.

[13] *See Bolstering the Government's Cybersecurity: A Survey of Compliance with the DHS Directive*, *supra*, *available at* https://science.house.gov/legislation/hearings/subcommittee-oversight-hearing-bolstering-government-s-cybersecurity-survey.

Pre-deprivation process would have been a valuable safeguard against an erroneous, unnecessary, and overly-broad debarment. Instead, and notwithstanding Kaspersky Lab's offer to do so, DHS simply refused to engage with Plaintiffs at all prior to the issuance of the BOD. Affording Kaspersky Lab notice and an opportunity to be heard *prior* to the issuance of the BOD would have engendered a meaningful process by which Kaspersky Lab could have engaged DHS to consider, among other things, certain mitigating measures that would have addressed DHS's concerns or other alternative measures less severe than an outright ban.

Pre-deprivation process would also have been particularly valuable because the underlying statutory structure on which the BOD relies is devoid of any procedural safeguards or any identifiable process whatsoever. In fact, this action calls into question whether Congress ever intended FISMA to be used to initiate debarment proceedings against individual companies, as opposed to, for example, a vehicle to impose consistent, but generalized, security standards across the whole of government. Plaintiffs contend that such an approach by DHS would have been far more effective in protecting federal information systems (DHS's purported intent in issuing the BOD), rather than singling out and banning Kaspersky Lab products which function similarly to the products of many other vendors.

Specifically, while FISMA expressly provides for binding operational directives as a means of "safeguarding Federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk," *see* 44 U.S.C.§ 3552(b)(1), the statute nowhere provides for notice or any means to contest a compulsory directive by DHS. *See, e.g., Nat'l Council of Resistance of Iran v. Dep't of State*, 251 F.3d 192, 196 (D.C. Cir. 2001)("*NCRI*")("The unique feature of th[e] statutory procedure is the dearth of procedural participation and protection afforded the designated entity.").

The "procedure" offered by DHS stands in stark contrast to the procedures and protections afforded in a traditional FAR debarment—DHS's own basis for comparison. *See* Acting Secretary Decision Memo, Sept. 13, 2017 at AR 631 [Ex. D]. Under the FAR, debarring officials must provide formal notice of proposed suspension and/or debarment, including: (1) the reasons for the proposed debarment in terms sufficient to put the contractor on notice of the alleged conduct upon which the action is based, (2) notice of the opportunity to submit information and arguments in opposition to the proposed debarment within 30 days of receipt of the notice, (3) procedures that will govern the agency's decision-making process, and (4) the effects of proposed and actual debarment. *See* 48 C.F.R. Part 9.406-3(c). Critically, the debarring official's decision may be made only within 30 working days *after* receipt of information and argument from the contractor. *See* 48 C.F.R. Part 9.406-3(d)(1). This final protection under the FAR is consistent with the due process requirement that affected parties be given a meaningful opportunity to rebut the evidence before action is taken to deprive it of a property or liberty interest. By using FISMA in an unprecedented manner to effect a debarment, DHS is circumventing the FAR's procedural protections but with a far more draconian (and unconstitutional) result. At a minimum, the same safeguards provided for in the FAR should apply here.

c. The Government's Interest in Eliminating Alleged "Information Risks" and "Threats to U.S. National Security" Does Not Justify the Lack of Pre-Deprivation Due Process.

Under the third and final *Mathews* factor, DHS has failed to demonstrate how prior notice to Kaspersky Lab would have interfered with its goals of eliminating the alleged "information risks" and defeating "threats to U.S. national security," or why DHS failed to consider potential mitigation as a means to ensure that the BOD would not be overbroad or more severe than necessary. As explained below, the D.C. Circuit is unequivocal that national security and similar

concerns do not amount to a free pass relieving the government of its obligation to provide pre-deprivation process.

DHS's interest in eliminating alleged information security threats has no bearing on the *timing* of process. This is because of the critical difference between the "what" and "when" of due process, as set out in a judicial challenge to a terrorist designation:

> As to the third *Mathews v. Eldridge* factor…the Secretary rightly reminds us that no governmental interest is more compelling than the security of the nation. It is on this very point that the Secretary most clearly has failed to distinguish between the what of the Due Process Clause and the when. Certainly the United States enjoys a privilege in classified information affecting national security…[which] clearly affects the nature—the "what" of the due process which must be afforded petitioners. It is not immediately apparent how that affects the "when" of the process—that is, whether due process may be effectively provided post-deprivation as opposed to pre-deprivation.

NCRI, 251 F.3d at 207. Indeed, in *NCRI*, where the plaintiff challenged its designation as a foreign terrorist organization ("FTO") by the State Department, the D.C. Circuit held with respect to the third *Mathews* factor: "It is simply not the case...that the Secretary has shown how affording the organization whatever due process they are entitled to *before* their designation as foreign terrorist organization and the resulting deprivation of right would interfere with the Secretary's duty to carry out foreign policy." *Id*. at 207-208 (emphasis added). The D.C. Circuit contemplated the following hypothetical pre-deprivation notice and found it was "not immediately apparent" how providing it would work any harm to the government's interest in national security:

> We are considering designating you as a foreign terrorist organization, and in addition to classified information, we will be using the following summarized administrative record. You have the right to come forward with any other evidence you may have that you are not a foreign terrorist organization.

Id. at 208.

Building on *NCRI*, the D.C. Circuit in *People's Mojahedin Organization of Iran v. Dep't of State*, 613 F.3d 220, 228 (D.C. Cir. 2010)("*PMOI*") held that the State Department violated a designated terrorist organization's Fifth Amendment due process rights with respect to its petition for revocation of its redesignation as a terrorist organization: "[W]e have held due process requires that the PMOI be notified of the unclassified material on which the Secretary proposes to rely and an opportunity to respond to that material *before* its redesignation" as an FTO. (emphasis in original). But "[t]he PMOI was notified of the Secretary's decision and permitted access to the unclassified portion of the record only *after* the decision was final." *Id*. at 227. (emphasis in original).

More recently, in *Ralls*, the D.C. Circuit applied this same analysis in the context of a Presidential Order which resulted in deprivation of a property interest by prohibiting a proposed transaction on national security grounds. 758 F.3d at 318-322. The D.C. Circuit held the absence of pre-deprivation process unconstitutional—even where the second *Mathews* factor was unclear: "As the FTO cases make plain, a substantial interest in national security supports withholding only the *classified* information but <u>does not excuse the failure to provide notice of,</u> and access to, the unclassified information used to prohibit the transaction." *Id*. at 320 (underlined emphasis added).

Simply put, "the fundamental norm of due process clause jurisprudence requires that *before* the government can constitutionally deprive a person of the protected liberty or property interest, it must afford him notice and hearing." *NCRI*, 251 F.3d at 205 (emphasis added); *Ralls*, 758 F.3d at 318 ("Due process ordinarily requires that procedures provide notice of the proposed official action and the opportunity to be heard at a meaningful time and in a meaningful manner.")(internal quotation omitted).

Due process's "root requirement [is] that an individual be given an opportunity for a hearing *before* he is deprived of any significant property interest, except for extraordinary situations where some valid governmental interest is at stake that justifies postponing the hearing until after the event." *Boddie v. Connecticut*, 401 U.S. 371, 379 (1971)(underlined emphasis added). Specifically, "where a State must act quickly, or where it would be impractical to provide predeprivation process, postdeprivation process satisfies the requirements of the Due Process Clause." *Gilbert v. Homar*, 520 U.S. 924, 930 (1997)(citations omitted). S*ee also, FDIC v. Mallen*, 486 U.S. 230, 240 (1988)(an "important government interest, accompanied by a substantial assurance that the deprivation is not baseless or unwarranted, may in limited cases demanding prompt action justify postponing the opportunity to be heard until after the initial deprivation."). However, "absent such exceptional circumstances, the law [is] clearly established that publication of stigmatizing information without a name-clearing hearing violates due process." *Cleanmaster Indus., Inc. v. Shewry*, 491 F. Supp. 2d 937, 946 (C.D. Cal. 2007)(internal quotation omitted)(alteration in original).

Here, nothing in the record suggests an "extraordinary situation," or indicates that the "State must act quickly," or that " it would be impractical to provide predeprivation process," or that this is one of those "limited cases demanding prompt action." Pre-deprivation process would in no way inhibit the government's interest in security in contrast to, for example, the forfeiture context where funds or property may swiftly be disposed of. *See, e.g., United States v. James Daniel Good Real Prop.*, 510 U.S. 43, 52 (1993)(explaining that "[t]he ease with which an owner could frustrate the Government's interests in the forfeitable property created a special need for very prompt action that justified the postponement of notice and hearing until after the seizure"—specifically the property at issue (a yacht) was the "sort of property that could be

removed to another jurisdiction, destroyed, or concealed, if advance warning of confiscation were given").

Neither the BOD, the Decision, the BOD Information, the Final Decision, nor the Final Information even consider whether the "information security risks" allegedly presented by Kaspersky Lab are imminent, exigent, or urgent, much less to a degree that would justify sacrificing pre-deprivation notice. *See* AR 633-35 [Ex. C], AR 628-32 [Ex. D], AR 3- 24 [Ex. E], AR 934-37 [Ex. J], and AR 752-76 [Ex. K]. Far from evidencing any urgency, DHS provides *three months* for affected agencies to "begin to implement the agency plan of action." *See* AR 635 [Ex. C]. Relatedly, the BOD relies heavily on media accounts, some nearly two years old, hardly indicating a paramount need for swift action. *See, e.g.*, AR 10, n.25 (Fox News), AR 12-13, n.38, 40, 42, and AR 20, n.59 (Bloomberg) [Ex. E].

In fact, urgency and immediacy are conspicuously absent from the reasons DHS gives for relying on the BOD rather than the traditional debarment procedure under the FAR. *See* AR 631 [Ex. D]. Rather, as explained *supra*, the Decision explains that DHS considers the BOD to be a more "appropriate" process than a debarment proceeding under the FAR principally because it is more extensive and severe. *Id*.

DHS had ample time and opportunity to engage with Plaintiffs prior to the issuance of the BOD, as was constitutionally required. Plaintiffs themselves contacted DHS in July offering to engage with the department. AR 749-50 [Ex. A]. DHS not only ignored their obligation to notify and hear Plaintiffs prior to the issuance of the BOD, they expressly rejected it by ignoring Plaintiffs' offer. AR 940 [Ex. B].

d. The *Mathews* Factors Weigh in Favor of Pre-Deprivation Process.

In *Ralls*, notwithstanding doubts about the second *Mathews* factor (risk of an erroneous deprivation, and the probable value of additional or substitute procedural safeguards) and despite the government's legitimate national security interest, the D.C. Circuit held that the absence of pre-deprivation process was a *clear* constitutional violation: "This lack of process constitutes a clear constitutional violation, notwithstanding the [government's] substantial interest in national security and *despite our uncertainty that more process would have led to a different presidential decision*." *Ralls*, 785 F.3d at 320 (emphasis added). It is no different here. The *Mathews* factors collectively clearly favor pre-deprivation notice and a process consistent with the "fundamental norm" of due process. *NCRI*, 251 F.3d at 205.

2. Kaspersky Lab Should Have Been Afforded an Opportunity to Respond to the Maggs Report.

Kaspersky Lab's due process rights were also violated because the Company had insufficient notice of the Maggs Report on Russian law and was therefore deprived of a meaningful opportunity to rebut it. As referenced above, rather than introducing the Maggs Report with the September 13, 2017, BOD, which would have enabled Plaintiffs to address and/or rebut the report when Plaintiffs filed the Kaspersky Lab Submission, DHS produced the report with its December 6, 2017, Final Decision in an apparent attempt to bolster their decision making after the fact. AR 752 [Ex. K], AR 777-821 [Ex. M]. In so doing, DHS foreclosed Plaintiffs any opportunity to rebut or contest it, in violation of their Fifth Amendment due process rights. *See Ralls,* 758 F.3d at 319 ("due process requires, at the least, that an affected party…be given access to the unclassified evidence on which the official actor relied and be afforded an opportunity to rebut that evidence."); *PMOI*, 613 F.3d at 227 (finding due process

violation where agency failed to provide notice of evidence on which it relied before final decision).

Had Plaintiffs had timely notice of the Maggs Report, they would have contested its conclusions including, for example, that under Russian law Kaspersky Lab is considered an "organizer of the dissemination of information on the Internet." AR 779 [Ex. M]. From this erroneous conclusion, the Maggs Report incorrectly determines that Kaspersky Lab's antivirus software is subject to Russia's surveillance laws aimed at detecting and preventing terrorism and other criminal activities. *See, e.g.*, AR 782-84, AR 792-93 [*Id*.] DHS's (initial) Decision and the BOD Information asserted more generalized arguments about Russian law (s*ee* AR 14-16 [Ex. E]), which Plaintiffs addressed in the Kaspersky Submission.

If Plaintiffs had notice, they also would have argued that the author of the Maggs Report is unqualified to draw these conclusions in any event. Professor Maggs is not a Russian lawyer. His curriculum vitae makes clear that he has never been admitted to practice law in Russia, and indeed, he never has practiced law in Russia. *See* AR 777-78 (¶¶ 1-10) and AR 794-821 [Ex. M]. This is important, as he draws conclusions based on his own subjective interpretation of Russian law. *See, e.g.,* AR 792 [*Id*.] ("Therefore, *I do not believe* that the [Russian Federal Security Service] would need to obtain any court order to use SORM technologies to intercept data transmissions...")(emphasis added).

Plaintiffs therefore also establish a due process violation, and hence an APA claim, based on the absence of opportunity to rebut the Maggs Report, and other matters raised for the first time in the Final Decision and its Final Information.

II. The BOD is Subject to APA Review, is Unsupported by Substantial Evidence and is Arbitrary and Capricious

Nor does the BOD survive Plaintiffs' non-constitutional claim under APA review. As set out below, the BOD is subject to APA review, is not backed by substantial evidence, and is therefore arbitrary and capacious.

A. Binding Operational Directives Issued under FISMA are Subject to APA Review.

This case presents the first judicial challenge to a FISMA binding operational directive. The APA applies here because FISMA does not specify its own standard of review. *See Chu v. CFTC*, 823 F.3d 1245, 1250 (9th Cir. 2016)("Where Congress does not specify a standard of review, an agency's factual findings are reviewed for substantial evidence under the [APA]")(citation omitted), *accord*, *Witter v. CFTC*, 832 F.3d 745, 749 (7th Cir. 2016).

The decision to issue a binding operational directive under FISMA does not fall within the narrow "committed to agency discretion" exception of the APA. *See* 5 U.S.C. § 701(a)(2). The APA embodies the basic presumption of judicial review to one suffering legal wrong because of agency action, or adversely affected or aggrieved by agency action within the meaning of a relevant statute." *Delta Air Lines v. Export-Import Bank of the U.S.*, 718 F.3d 974, 976 (D.C. Cir. 2013)(internal quotations omitted). Thus, as a threshold matter, "[t]he exception for agency action 'committed to agency discretion by law' is a very narrow one, reserved for those rare instances where statutes are drawn in such broad terms that in a given case there is no law to apply." *Hi-Tech Furnace Systs., Inc. v. FCC*, 224 F.3d 781, 788 (D.C. Cir. 2000)(internal quotation and citation omitted). Rather, "there is a strong presumption that agency action is reviewable and Congress rarely draws statutes in terms so broad that there is no meaningful standard." *Kirwa v. DOD*, 2017 U.S. Dist. LEXIS 176826, at *28 (D.D.C. Oct. 25, 2017),

quoting Sec'y of Labor v. Twentymile Coal Co., 456 F.3d 151, 156 (D.C. Cir. 2006). "To determine whether an action is committed to agency discretion courts consider both the nature of the administrative action at issue and the language and structure of the statute that supplies the applicable legal standards for reviewing that action." *American Petroleum*, 943 F. Supp. 2d at 66 (quotation omitted).

First, the BOD clearly is not one of the "categories of administrative decisions" that the Supreme Court and the D.C. Circuit consider presumptively unreviewable—for example, an agency's refusal to take enforcement action. *Secretary of Labor v. Twentymile Coal Co.*, 456 F. 3d 151, 156 (D.C. Cir. 2006). Rather, as DHS makes clear in both its Information and Decision Memos, the BOD has effectuated a debarment. *See* AR 5-6 [Ex. E] and AR 631 [Ex. D], sections entitled "**DEBARMENT.**" And, as the D.C. Circuit held long ago, debarments must be subject to APA review:

> The command of the Administrative Procedure Act is not a mere formality. Those who are called upon by the government for a countless variety of goods and services are entitled to have notice of the standards and procedures which regulate these relationships...Disqualification from bidding or contracting…directs the power and prestige of government at a particular person and, as we have shown, may have a serious economic impact on that person. Such debarment cannot be left to administrative improvisation on a case-by-case basis. The governmental power must be exercised in accordance with accepted basic legal norms. Considerations of basic fairness require administrative regulations establishing standards for debarment and procedures which will include notice of specific charges, opportunity to present evidence and to cross-examine adverse witnesses, all culminating in administrative findings and conclusions based upon the record so made.

Gonzalez, 334 F.2d at 578.

Next, Congress need only "provide[] a meaningful—not a rigorous, but neither a meaningless—standard against which to judge the exercise of agency discretion." *Arent v. Shalala*, 70 F.3d 610, 614 (D.C. Cir. 1995). The limitation of the BOD to "safeguard" federal IT systems from "a known or reasonably suspected information, security threat, vulnerability, or

risk" certainty provides "meaningful standards" against which to measure DHS's action. 44 U.S.C. §§ 3552(b)(1), 3553(b)(2). These statutory limits "do[] not provide [DHS] unbridled discretion to [debar]." *See Am. Petroleum*, 943 F. Supp. at 68.

B. The BOD is Unsupported by Substantial Evidence and is Arbitrary and Capricious.

Under the "arbitrary and capricious" standard in 5 U.S.C. § 706(2)(A), the Court must reverse an agency's decision not supported by substantial evidence. *See, e.g., Safe Extensions, Inc. v. FAA*, 509 F.3d 593 (D.C. Cir. 2007). The BOD fails to satisfy this standard because substantial evidence does not support DHS's conclusion "that Kaspersky-branded products present a known or reasonably suspected information security threat, vulnerability, or risk to Federal information and information systems." AR 631 [Ex. D].

1. The BOD Information is Based Almost Exclusively on Uncorroborated News Reports.

Rather than relying on its own fact-finding, DHS's principal and overwhelming source of "evidence" in the BOD Information is uncorroborated news reports.[14] In a particularly stark contradiction after the fact, Jeanette Manfra, the DHS author of the memoranda in support of the BOD and the Final Decision, testified before the House Committee on Science, Space, and Technology on November 14, 2017, that, in relation to allegations against Plaintiffs, she could not "make a judgement based off of press reporting."[15] Yet that is precisely what she asked DHS's Acting Secretary to do in her memoranda recommending the BOD.

Although the D.C. Circuit has found in limited instances that media reports may be relied upon to establish discrete facts, DHS has taken a great leap here by using media reports to

[14] *See* AR 3-24 [Ex. E], citations to: Rachel Maddow Show at AR 9, n.17; AR 12-13, n.37; AR 16, n.50; AR 22, n.66; Fox News at AR 10, n.25; Wired Magazine at AR 11, n.28, 31; AR 12, n.34, 37; AR 14, n.45, 46; AR 20, n.58; Bloomberg at AR 12, n.32, 33; AR 13, n.38, 39, 40, 42; AR 20, n. 59; Forbes at AR 20-21, n.61.

[15] *See Bolstering the Government's Cybersecurity*, *supra*, p. 24.

connect loose allegations with key legal conclusions. *See, e.g., Zevallos v. Obama,* 793 F.3d 106, 112 (D.C. Cir. 2015)(reliance on newspaper articles that a designated drug kingpin controlled overseas assets). For example, in *Holy Land Foundation v. Ashcroft*, 333 F. 3d 156, 162 (D.C. Cir. 2003), the D.C. Circuit made clear that, while the terrorist designation could be based on "a broad range of evidence, including intelligence data and hearsay declarations"—Treasury's decision "was based on ample evidence in a *massive* administrative record"—including "testimony of numerous FBI sources and findings by both Israeli and Palestinian governmental authorities." (emphasis added).

In contrast, many sections of the BOD Information and key DHS findings in support of the BOD's are supported exclusively by uncorroborated news reports. This is true for all three core reasons which DHS relies upon: (1) 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;[16] (2) Ties between certain Kaspersky officials and Russian intelligence and other government agencies;[17] and (3) Russian legal provisions that allow Russian intelligence agencies to request or compel assistance from Kaspersky and to intercept communications transiting Russian networks.[18] Fayhee Decl. Ex. A at 1. The second of these—alleged "ties between certain Kaspersky officials and Russian intelligence and other government agencies"—is the most critical. The reliance on media sources is simply misplaced and is a wholly inadequate substitute for careful and judicially reviewable agency fact-finding.

Finally, DHS alludes to the classified record in an apparent attempt to distract from the deficiencies in the public administrative record upon which its decision must (and is claimed to)

[16] *See, e.g.*, AR 8, nn.14-16, AR 9, n.17, AR 10, n. 25 [Ex. E].
[17] *See, e.g.,* AR 11, nn.29-31; AR 12, nn. 32-33 and 37; AR 13, nn. 38-40 and 42. [Ex. E]
[18] *See, e.g.*, AR 14, n46 AR 16, nn. 49-50 [Ex. E]

be based. AR 631 [Ex. D]. DHS does so, as if the existence of such a record, regardless of its content, lends weight to their arguments on national security grounds, insinuating that if only we were to pull back the curtain all potential questions and concerns would be satisfied.

2. NCCIC Reports Lack Technical Rigor and Specificity to Plaintiffs' Products.

DHS also seeks to rely on an internal report by the National Cybersecurity and Communications Integration Center ("NCCIC") in technical support of the BOD. *See* AR 25-32 [Ex. N]. The NCCIC falls under DHS' jurisdiction and its report can hardly be considered an independent assessment or the product of an informed, deliberative, interagency review. The BOD Information itself is predominately non-technical in nature and focuses on rumors and speculation that Kaspersky Lab has ties to the Russian government, rather than on the technical risks or merits of Kaspersky software relative to other anti-virus software in use by the U.S. federal government. The NCCIC Assessment outlines general theoretical information security risks associated with the use of modern anti-virus software; however, DHS has presented no evidence to demonstrate either that (i) NCCIC performed a sufficient technical analysis of Kaspersky Lab products, or (ii) Kaspersky Lab products have been used for any improper purpose.

In order to address the concerns raised in the BOD regarding the capabilities and alleged vulnerabilities of Kaspersky Lab's products, Plaintiffs, through counsel, retained cybersecurity professionals at computer and software forensics company Berkley Research Group, LLC ("BRG") to: (i) review the technical methodology employed by DHS in its issuance of the BOD; and (ii) provide an independent expert review and assessment of any technical information security risks described in the BOD or its supporting materials.

BRG concluded that neither the NCCIC Assessment nor the BOD Information provide any technical evidence to indicate that any Kaspersky Lab products represent "either a greater or lesser technical risk to federal information systems than similar anti-virus software products, vendors, or services." AR 694 [Ex. I]. Rather, BRG's technical analysis concluded that other anti-virus software products (not subject to the BOD) are likely just as vulnerable to theoretical exploitation by malicious cyber actors as DHS alleges is the case for Kaspersky Lab software products.

The NCCIC Assessment was clearly commissioned by DHS for the sole purpose of supporting the BOD. DHS also introduced a "Supplemental Assessment" by the NCCIC together with the Final Decision in another attempt to bolster and shore up the pre-determined outcome recorded in the Final Decision. AR 822-32 [Ex. O]. As with the Maggs Report (discussed above), Plaintiffs have had no opportunity through the confines of DHS's inadequate process to respond to the findings of the NCCIC Supplemental Assessment.

Tellingly, Manfra publicly and specifically testified that the government *does not have conclusive evidence* that Kaspersky Lab had facilitated the breach of any U.S. government information system.[19] In light of this fact, in its Final Decision and at the conclusion of its purported process, DHS claims for the first time that no evidence of any such breach or wrongdoing is required. AR 760 [Ex. K] ("No Need for Evidence of Wrongdoing."). In so doing, DHS disclaims the need for any evidentiary support whatsoever but asks the Court to sustain the debarment nonetheless.

[19] *See Bolstering the Government's Cybersecurity: A Survey of Compliance with the DHS Directive*, *supra*, p. 19.

CONCLUSION

Plaintiffs have shown that the issuance of the BOD violated their Fifth Amendment due process rights, and was arbitrary and capricious. Plaintiffs therefore respectfully request that the Court declare the BOD invalid, order its rescission, and enjoin its enforcement permanently. Plaintiffs further request that the Court remand to DHS for further proceedings, directing the agency to use a process compliant with Fifth Amendment procedural due process requirements, and the evidentiary requirements of the APA.

Dated: February 22, 2018

Respectfully submitted,

/s/ Ryan P. Fayhee
Ryan P. Fayhee (Bar No. 1033852)

/s/ Steve Chasin
Steven Chasin (Bar No. 495853)

Baker & McKenzie LLP
815 Connecticut Avenue NW
Washington D.C. 20006
Tel: (202) 452 7024
Fax: (202) 416 7024
Ryan.Fayhee@bakermckenzie.com
Steven.Chasin@bakermckenzie.com

Attorneys for Kaspersky Lab, Inc. and Kaspersky Labs Limited