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' APPLICATION FOR PRELIMINARY INUNCTION

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

INTRODUCTION

On September 13, 2017, the U.S. Department of Homeland Security (DHS) issued Binding Operational Directive 17-01 ("the BOD") which branded the antivirus software developed by Plaintiffs Kaspersky Lab, Inc. and Kaspersky Labs Limited (collectively, "Kaspersky Lab" or the "Company") an "information security risk[]" to U.S. Government information systems, and summarily ordered its removal from those systems and permanent debarment. The BOD effected this debarment immediately, although DHS deemed the BOD "final" about three months later on December 6, 2017. DHS did not provide Plaintiffs prior notice of the BOD, nor a prior opportunity to contest the purported evidence underlying it. Plaintiffs filed this action seeking rescission of the BOD, and now move for a preliminary injunction to stem the continuing significant damage to Kaspersky Lab's reputation and the loss of sales resulting from the BOD.

As former Chief Justice Warren Burger explained, a debarment "directs the power and prestige of government at a particular person and . . . may have a serious economic impact on that person." *Gonzalez v. Freeman*, 334 F.2d 570, 578 (D.C. Cir. 1964). Thus, "the resolution of debarment cases is a serious matter that has an immediate and profound effect on the particular individuals involved." *Canales v. Paulson*, 2007 U.S. Dist. LEXIS 50924, at *14 n.1 (D.D.C. July 16, 2007) (internal quotation omitted). The BOD has had exactly that impact on Plaintiffs; not only precluding their ability to do business with the U.S. Government, but also significantly damaging Plaintiffs' reputation and consequently their commercial and consumer business. DHS used the BOD to achieve a preordained result—the immediate debarment of Kaspersky Lab, and the consequential and foreseeable adverse effect on its U.S. commercial sales. As explained below, the BOD achieved this result while depriving Kaspersky Lab of any

meaningful or constitutionally sound process to challenge the tenuous, often anonymous, and uncorroborated media stories and other self-serving public statements which DHS relied upon to justify its action.

The BOD was issued pursuant to the Federal Information Security Modernization Act of 2014 ("FISMA") 44 U.S.C. § 3551 *et seq*. (2014). This provision 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). The BOD ordered the identification, removal, and discontinuation of Kaspersky Lab software by all U.S. government agencies, as well as private contractors operating within their IT systems. This debarment violated Plaintiffs' Fifth Amendment rights, by depriving Kaspersky Lab of a constitutionally protected liberty interest without due process of law, and therefore should not withstand Administrative Procedure Act ("APA") review. At the very least, the Fifth Amendment required DHS to give Plaintiffs notice and a meaningful opportunity to contest DHS's "evidence" *before* issuance of the BOD. No such notice or opportunity was afforded to Plaintiffs.

The BOD professed to provide due process through a staged 30-60-90 day implementation structure (explained in further detail below), but this process was illusory and did not meet minimum due process standards. In reality, the debarment of Plaintiffs and the resulting damage was immediate and complete *upon the issuance* of the BOD. The process for identification, removal, and discontinuation began immediately and unfairly prejudiced government agencies—alongside private and commercial consumers—against Plaintiffs' software. In fact, 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.

DHS's professed "administrative process" only gave Plaintiffs an opportunity to respond to the BOD *after* it effected the debarment on September 13, 2017. Following this process, Plaintiffs filed a lengthy written submission with DHS on November 10, 2017, challenging the BOD and attempting to change the result (the "Kaspersky Lab Submission"). DHS rejected that submission in a perfunctory and undeveloped analysis in a "Final Decision" dated December 6, 2017, which maintained the BOD without modification—just ahead of the 90-day mark.

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. Accordingly, DHS has failed to demonstrate Plaintiffs' software presented such an "extraordinary situation" necessary to justify postponement of due process until after the deprivation of a protected interest. *See Boddie v. Connecticut*, 401 U.S. 371, 379 (1971).

The BOD also fails to meet the evidentiary requirements of the APA. As a remarkable and unprecedented substitute for the agency fact-finding process, DHS's principal and overwhelming source of "evidence" is uncorroborated and sometimes anonymously sourced news reports—including, among others, the Rachel Maddow Show, Fox News, Wired Magazine, Bloomberg News, and Forbes. DHS characterizes these reports as "a substantial body of evidence"—but none of it comes close to meeting the APA's "substantial evidence" burden. Indeed, DHS admits in its Final Decision that it *has no evidence of any security breach or related wrongdoing* by Plaintiffs. Relatedly, 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." Yet that is precisely what she asked DHS's Acting Secretary to do in her memoranda recommending the BOD.

The Court should grant this application, and preliminarily rescind the BOD. As set out in detail below, Plaintiffs establish a likelihood of success on both of their APA claims—although a showing on only one is necessary: (1) violation of Plaintiffs' Fifth Amendment right to due process, and (2) arbitrary & capricious decision-making, unsupported by substantial evidence. Absent more immediate relief, the BOD will continue to perpetuate irreparable harm to Plaintiffs' reputation, leading to continued significant losses to U.S. sales, and those abroad. Indeed, as a direct result of this and related government action, major U.S. retailers have pulled Kaspersky Lab products from their shelves. The Company just closed and finalized its financial results for Fiscal Year 2017 on January 17, 2018, and they show that Kaspersky Lab, Inc.'s gross bookings from U.S. retail sales in Q4 2017 *fell 61%* compared to the same period in 2016. Likewise, the company's gross bookings from U.S. retail sales in the second half of 2017 *fell 50%* compared to the same period in 2016. The Company's U.S. sales results in the business-to-business segment also show a significant and unprecedented decline in the period following the BOD, with a 45% drop in Q4 2017 compared to the same period in 2016. Finally, the balance of equities and public interest weighs in Kaspersky Lab's favor given the clear constitutional violation, and particularly where the responsible government officials have acknowledged that there is no conclusive evidence that Kaspersky Lab has directed or facilitated any information security breach, and have indicated their desire to harm Plaintiffs' commercial interests.

STATEMENT OF FACTS

I. Background

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*. Among its offices are research and development centers employing anti-malware experts in the U.S., Europe, Japan, Israel, China, Russia, and Latin America. *Id*. . 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 ¶ 10. Mr. Kaspersky has been the CEO of Kaspersky Lab since 2007. *Id*. Although the Company's global headquarters are in Moscow, more than 85% of its sales in 2016 were 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*.

Plaintiff Kaspersky Lab, Inc. is a Massachusetts corporation based in Woburn, Massachusetts, and serves as the North American headquarters of Kaspersky Lab. *Id*. at ¶ 4. Kaspersky Lab, Inc. is a direct wholly-owned subsidiary of its U.K. parent, Plaintiff Kaspersky Labs Limited. *Id*.

The U.S. has been one of the most significant geographic markets in Kaspersky Lab's global business. *Id*. at ¶ 11. Sales to customers in the U.S. represented approximately one quarter of total global bookings in 2016. *Id*.

A tiny fraction of Kaspersky Lab sales in the U.S. have been to the U.S. Government, and have been driven by channel sales through (independent) resellers. *Id*. at ¶ 13. Active

licenses held by federal agencies have 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*.

II. DHS Published the BOD without affording Kaspersky Lab Notice or an Opportunity to Heard

On July 18, 2017, Kaspersky Lab wrote to DHS, 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. Declaration of Ryan P. Fayhee ("Fayhee Declaration") Ex. A. DHS responded on August 14, 2017, acknowledging the Company's letter and its offer of assistance, and indicated that DHS "will be in touch again shortly." *Id*. Ex. B. DHS never was.

Rather, on September 13, 2017, DHS issued the BOD, without affording any notice to Kaspersky Lab or prior opportunity to rebut its allegations. *Id*. 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 reasonably suspected information security threat, vulnerability, or risk." *Id*. Ex. D at 1 (*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." *Id*. at 2.

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. at 2. The Decision 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." *Id.* at 4.

The Decision cites an internal 21-page DHS Information Memorandum, dated September 1, 2017 (the "BOD Information"), which DHS did not provide to Plaintiffs until September 29, 2017 (after the BOD had been issued and Plaintiffs notified), and then only following request of Plaintiffs' counsel. Fayhee Decl. ¶ 8, Ex. E. Jeanette Manfra, ("Manfra") Assistant Secretary for Cybersecurity and Communications, had authored the BOD Information, which was addressed to the then Acting DHS Secretary, through Chris Krebs, ("Krebs") Senior Official Performing the Duties of the Under Secretary. *Id.* Ex. E at 1. DHS also issued a letter to Eugene Kaspersky dated September 13, 2017, *id*. Ex. F, and issued a press release that same day accompanying the BOD. *Id*. Ex. G.

Based on the reasoning and allegations against Kaspersky Lab and its products made in the Decision and the BOD Information, 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."

BOD at *Id.* Ex. C at 2-3. ("30-60-90 days 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. *See* Decision at *Id.* Ex. F at 1. Accordingly, 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." *See* 82 Fed. Reg. 43,782, 43,784 (Sept. 19, 2017) at *Id*. Ex. H. DHS gave Plaintiffs until November 3, 2017 (subsequently extended to November 10, 2017) to respond to the BOD. *Id*. Ex. I. 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." *See* 82 Fed. Reg. 43,782, 43,784 (Sept. 19, 2017) at *Id*. Ex. H. But December 13 was one day *after* the 90-day deadline by which agencies were to have begun removing Kaspersky Lab products. In 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* Ex. L at 3 (*see* infra).

On November 10, 2017, Plaintiffs delivered to DHS the Kaspersky Lab Submission, an extensive written response to the BOD and its Information. *Id*. ¶ 13, Ex. J. 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 had 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. *Id*. ¶ 14.

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 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 on Kaspersky Lab. *Id*. Plaintiffs believe that such options were and are available to DHS and have not been fully explored either prior to or subsequent to the issuance of the BOD. *Id*. Ex. J. (Ex. 1 thereto)

On December 6, 2017, DHS issued a "Final Decision maintaining BOD 17-01 without modification." (the "Final Decision"). *Id*. Ex. K. at 1. 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"), *id*. Ex. L (including Exhibits 1-10), and a Letter to Eugene Kaspersky. *Id*. Ex. M.

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')." *Id*. Ex. L at 1 (Ex. 1 thereto). 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. *Id*. This foreclosed any opportunity for Plaintiffs to rebut or contest the Maggs Report, and other materials introduced at the time of the Final Decision.

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. Some 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. Some of them have gone ahead and just identified a way to remove the software so they're going about that."[1]

This testimony was 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.[2] Thus, federal agencies had begun removing Kaspersky Lab software long before

[1] *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* https://science.house.gov/legislation/hearings/subcommittee-oversight-hearing-bolstering-government-s-cybersecurity-survey.

[2] *Id*. at 53:11.

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, 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. N at p. 2 ("For the most part, we're closed out on removing the Kaspersky [antivirus]-branded products")(alternation in original).

Indeed, Amazon.com customer reviews clearly show that commercial and consumer opinions were prejudiced as soon as the BOD was issued in September 2017. *See* Fayhee Ex. O. 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 product:

> **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 pps. 1-2 (emphasis added).[3] Indeed, the BOD covers the same products used by commercial customers and individual customers, and so destroyed the reputation that those products enjoy with current and potential users. Gentile Decl. at ¶ 16.

DHS intended the BOD to have precisely this impact. In fact, Krebs stated DHS's intent bluntly during public statements on October 31, 2017: "[W]hen [DHS] makes a pretty bold

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

statement like issuing the Kaspersky binding operational directive I think that's a fairly strong signal [to consumers]."[4]

The BOD also 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 growing. Gentile Decl. at ¶¶ 18-25. 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 ¶ 20. Some of these retailers, which provided a steady stream of both new customers and consumer product subscription renewals to Kaspersky Lab over the years, went even further. *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*. As a result of these actions, 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 ¶ 21. 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 fall 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 ¶ 22. 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*. The license renewal rate of existing B2B customers has fallen 23 percentage points in the second half of 2017 compared to the same period in 2016. *Id*.

---

[4] *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/.

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 ¶ 23. In these cases, the potential B2B customers have 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 been successful in making sales of Kaspersky Lab products recently, the Company is receiving and processing an unprecedented volume of product return and early termination requests. *Id*. at ¶ 24. 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*. 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*.

V. National Defense Authorization Act for FY 2018

The BOD expressly excepts from its scope National Security systems. Fayhee Decl. Ex. C at 1. However, on December 12, 2017, President Trump signed into law the National Defense Authorization Act for FY 2018 ("NDAA") which prohibits the entire Federal Government from using any Kaspersky Lab software, *effective October 1, 2018*: "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…." Pub. Law No. 115-91, § 1634(a), (b). Thus, as DHS puts it: "[U]ntil October 1, 2018, the BOD's requirement

to start removal on Day 90, unless modified or rescinded by [DHS], *is the operative prohibition on agency use of Kaspersky products*." Final Information at Fayhee Decl. Ex. L at 5-6 (emphasis added).

Kaspersky Lab is currently considering legal recourse available to it with respect to the NDAA provision prior to its effective date. In the meantime, the BOD has, and continues to cause immediate and irreparable harm, which Plaintiffs seek to abate now through this Preliminary Injunction Application.

STANDING

Kaspersky Lab, Inc. and Kaspersky Labs Limited have standing to assert their APA claims. First, 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)).

Kaspersky Lab, Inc. clearly meets this standard: the company sold its products (through its partners) to the U.S. government—and the BOD now prohibits those sales. *See* Gentile Decl. ¶ 18; Fayhee Decl. Ex. C at 2. The company also has been injured by DHS's derogatory and inaccurate comments, made through the BOD, press release and statements made publicly by senior DHS personnel—and the resulting harm to the company's commercial sales. *See* Gentile Decl. ¶¶ 15-17, 19-24 .

Likewise, due to the adverse impact on its subsidiary, the U.K. parent Plaintiff Kaspersky Labs Limited 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, while sales to customers in the U.S. represented approximately one quarter of total global bookings in 2016, the U.S. accounted for only one fifth of total global bookings in 2017. Gentile Decl. ¶ 25. Plaintiff Kaspersky Labs Limited also has Article III standing based on (1) the BOD's preclusive effect—the BOD bars Kaspersky Labs Limited from selling to the U.S. government, and (2) the reputational harm caused globally to Kaspersky Labs Limited (and its other subsidiaries) from the labelling of all "Kaspersky products" as "information security risks." *See* Gentile Decl. ¶¶ 15-18; Fayhee Decl. Ex. C at 2; *Id.* Ex. G at 1.

With these injuries to both Plaintiffs, the other two Article III elements naturally follow. The injuries are fairly traceable to the BOD, and rescission of the BOD would likely redress these injuries. *See Spokeo*, 136 S. Ct. at 1547; *see* Gentile Decl. ¶¶ 14-27.

Kaspersky Labs Limited also satisfies prudential standing requirements—namely, the "shareholder standing rule," which "generally prohibits shareholders from initiating actions to enforce the rights of the corporation…" *See Franchise Tax Bd.*, 493 U.S. 331 at 336. "There is … an exception to [the shareholder standing] rule allowing a shareholder with a direct, personal interest in a cause of action to bring suit even if the corporation's rights are also implicated." *Id*. Specifically, "[t]o determine if a shareholder's claims are derivative of the corporation's claims for standing purposes and thus barred by the shareholder standing rule, courts apply the law of the state of incorporation." *Harpole Architects, P.C. v. Barlow*, 668 F. Supp. 2d 68, 76 (D.D.C. 2009)((internal quotation omitted).

Under the law of Massachusetts (Kaspersky Lab, Inc.'s state of incorporation), "[i]ndirect harms, suffered generally by all shareholders, must be brought derivatively, on behalf of the corporation." *In re AllianceBernstein Mut. Fund Excessive Fee Litig*., 2005 U.S. Dist. LEXIS

24263 (S.D.N.Y. Oct. 19, 2005), *vacated in part on other grounds*, 2006 U.S. Dist. LEXIS 939 (S.D.N.Y. Jan. 11, 2006)(citing *Jackson v. Stuhlfire*, 28 Mass. App. Ct. 924, 925 (1990)("[T]he wrong underlying a derivative action is *indirect*, at least as to the shareholders …. [i]t adversely affects them merely as they are the owners of the corporate stock; only the corporation itself suffers the direct wrong.")(internal quotation omitted)). Here, the two harms described above—the BOD's preclusive effect, and the BOD's reputational harm—are "direct wrong[s]" to Kaspersky Labs Limited, and therefore are not derivative of the subsidiary Kaspersky Lab, Inc.'s claims. *See Id*. Accordingly, Kaspersky Labs Limited meets the exception to the shareholder standing rule, and has satisfied prudential standing requirements.

Relatedly, Kaspersky Labs Limited also 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 assert Fifth Amendment due process protections because of its "substantial connections with this country"—reviewing the record as a whole, and 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 protection. See *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, 26. Sales to customers in the U.S., through the Massachusetts subsidiary, represented approximately one quarter of total Kaspersky Lab global bookings in 2016, and one fifth of total global bookings in 2017. *Id*. at ¶ 25. 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. These are clearly "substantial connections" to this country, and support Kaspersky Labs Limited's standing to assert a violation of constitutional due process, through its APA claim.

LEGAL STANDARD FOR PRELIMINARY INJUNCTION

A preliminary injunction grants "intermediate relief of the same character as that which may be granted finally." *De Beers Consol. Mines v. United States*, 325 U.S. 212, 220 (1945). "A plaintiff seeking a preliminary injunction must establish (1) that he is likely to succeed on the merits, (2) that he is likely to suffer irreparable harm in the absence of preliminary relief, (3) that the balance of equities tips in his favor, and (4) that an injunction is in the public interest." *Winter v. Natural Res. Def. Council, Inc*., 555 U.S. 7, 20 (2008); *Pursuing Am.'s Greatness v. FEC*, 831 F.3d 500, 505 (D.C. Cir. 2016). The final two factors "'merge when the Government is the opposing party,'" as in this case: the "[agency's] harm and the public interest are one and the same, because the government's interest is the public interest." *Id*. at 511 (*quoting Nken v. Holder*, 556 U.S. 418, 435 (2009)).

"The four factors have typically been evaluated on a sliding scale. Under this sliding-scale framework, if the movant makes an unusually strong showing on one of the factors, then it does not necessarily have to make as strong a showing on another factor." *Doe v. Trump*, 2017 U.S. Dist. LEXIS 178892, *44 (D.D.C. Oct. 30, 2017)(J. Kollar-Kotelly)(internal quotation

omitted).[5] Thus, using the sliding scale, "a court may issue injunctive relief upon a particularly strong likelihood of success on the merits even if there is a relatively slight showing of irreparable injury." *Alf v. Donley*, 666 F. Supp. 2d 60, 69 (D.D.C. 2009)(internal quotation omitted)(granting preliminary injunction against debarment, explaining "in light of the fact that the plaintiff has made a strong showing of likelihood of success on the merits, he need make only a relatively small showing of irreparable harm to be entitled to injunctive relief.").

ARGUMENT

I. Plaintiffs have a Likelihood of Success on the Merits on Both of their APA Claims.

"Where multiple causes of action are alleged, plaintiff need only show likelihood of success on one claim to justify injunctive relief." *Kirwa v. U.S. Dep't of Def.*, 2017 U.S. Dist. LEXIS 176826, *27 (D.D.C. Oct. 25, 2017)(internal quotation omitted). As set out in detail below, Plaintiffs establish a high likelihood of success on both of their APA claims, even if a showing on either suffices.

A. Plaintiffs are Likely to Succeed on their Fifth Amendment Due Process Claim.

Plaintiffs' first claim is that the BOD violates their Fifth Amendment due process rights, and therefore violates the APA. "[T]he court's review of [this] constitutional challenge[] to agency action[]... is *de novo*." *Poett v. United States*, 657 F. Supp. 2d 230, 241 (D.D.C. 2009)(J. Kollar-Kotelly)("A reviewing court owes no deference to the agency's pronouncement on a constitutional question, and must instead make an independent assessment of a citizen's claim of constitutional right when reviewing agency decision-making.")

[5] *See also Id.* at n.5 ("[T]he D.C. Circuit has yet to hold definitively that *Winter* has displaced the sliding-scale analysis."). *See also, Advance Am. Cash Advance Ctrs., Inc. v. FDIC*, 2017 U.S. Dist. LEXIS 27887, *7 (D.D.C. Feb. 23, 2017) (notwithstanding *Winter*, the sliding-scale approach "remains good law in this Circuit.").

Specifically, "[t]o 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). Kaspersky Lab has a high likelihood of success on this claim because 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.

1. 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, (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. Fayhee Decl. Ex. C at 2. In fact, DHS dedicates an entire section entitled "**DEBARMENT**" in the Decision. *Id*. at Ex. D at 4. 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, 12 (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, the BOD labeled Kaspersky Lab's market-leading anti-virus products "information security risks" to U.S. Government information systems and summarily ordered their

identification, removal, and discontinuation by all subject U.S. government agencies. *Id*. at G at 1; *Id*. at C at 2-3. DHS's press release accompanying the BOD essentially alleges that Kaspersky Lab is an arm of Russian intelligences 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.

Id. at G at 1. These statements unquestionably impugn Kaspersky's Lab's reputation and integrity. Based on these stated concerns, as unsubstantiated as they may be, 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 exactly that—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, Kaspersky Lab's liberty interests are implicated and this element is therefore met.

2. The BOD's Procedures were Constitutionally Insufficient.

a. Pre-deprivation process was required under the *Mathews v. Eldridge* test.

Having deprived 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, 317-18 (D.C. Cir. 2014)(internal quotations omitted)(emphasis added). Specifically, pre-deprivation notice and an opportunity to be heard were required here based on 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 indicates that pre-deprivation process was required here.

1) Kaspersky Lab's Substantial Private Interest

Under the first *Mathews* factor, it is indisputable that Kaspersky Lab has a substantial private interest in its ability to sell its product to federal agencies, and in its reputation as a market-leading anti-virus software developer. *See* Gentile Decl. ¶¶ 15-16. It does not matter that quantitatively, Kaspersky Lab's sales (through its partners) to the U.S. government historically have been a small fraction of the company's total sales. *Id*. at ¶¶ 13, 16. Clearly, DHS's labelling of Kaspersky Lab's antivirus software products as "information security risks," its other derogatory remarks, and its summarily banning the Company from all government agencies—has a profound qualitative impact on the Company's brand, reputation, and prospects everywhere that it does business. See Fayhee Decl. at G; Gentile Decl. ¶ 16. Indeed, such harm was DHS's specific intent, as detailed above in the Facts (Section IV).

2) High Risk of an Erroneous Deprivation, and the Probable Value of Additional or Substitute Procedural Safeguards

With respect to the second *Mathews* factor, DHS simply refused to engage with Kaspersky Lab at all during the investigative phase preceding the BOD, which resulted in an erroneous deprivation. This was compounded by the highly technical nature of the subject. Affording Kaspersky Lab notice and an opportunity to be heard *prior* to issuance of the BOD would have engendered a meaningful process by which Kaspersky Lab could have engaged DHS to consider certain mitigation that would have addressed DHS's concerns or alternative measures less severe than an outright ban. That pre-deprivation process would have been a valuable safeguard against DHS's erroneous, unnecessary, and overly broad debarment.

Further, as explained below, the underlying statutory structure on which the BOD relies is devoid of any procedural safeguards or any identifiable process whatsoever. This calls into question whether Congress 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. This further indicates Defendants' true punitive intent against Plaintiffs in issuing the BOD.

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., Ralls*, 758 F.3d at 318 ("Notwithstanding the property interests potentially at stake, the statutory process by which the Secretary of State makes the FTO designation accords the FTO designee no procedural protections.")(*citing Nat'l Council of Resistance of Iran v. Dep't of State*, 251 F.3d 192, 196 (D.C. Cir. 2001) ("The unique feature of th[e] statutory procedure is the dearth of procedural participation and protection afforded the designated entity.")).

This is in stark contrast to the procedures and protections afforded in a FAR debarment—DHS's own basis for comparison. *See* Decision at Fayhee Decl. Ex. D at 4. 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.

Finally, the procedure which DHS did impose, *ad hoc,* necessarily involves a significant risk of erroneous deprivation of a liberty interest. As explained above, DHS expressly acknowledged that many agencies disregarded the 30-60-90 day structure, and began physical removal of the software before day 90, and further, many actually had completed removal by day 90 (rather than starting removal at that time). *See* Facts (Section IV), *supra*. The risk of erroneous deprivation is also manifest in the preordained nature of the outcome.

3) 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.

DHS's interest in eliminating these alleged threats simply does not affect the *timing* of process. The D.C. Circuit has explained the difference between the "what" and "when" of due process:

> 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.

Nat'l Council of Resistance of Iran v. Dep't of State, 251 F.3d 192, 207 (D.C. Cir. 2001) ("*NCRI*"). Indeed, in *NCRI*, where 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. 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 227.

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).

And 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 does not excuse the failure to provide notice of, 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). As the Supreme Court has stated, 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 pre-deprivation process, post-deprivation 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."). Simply put, "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 can 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").

The BOD, the Decision, the BOD Information, the Final Decision, and the Final Information all fail to even consider whether the "information security risks" allegedly presented

by Kaspersky Lab are imminent, exigent, or urgent—let alone to a degree that justify sacrificing pre-deprivation notice. *See* Fayhee Dec. Exs. C, D, E, K, L. Far from evidencing any urgency, DHS provides *three months* for affected agencies to "begin to implement their plan of action." *Id*. Ex. C at 3. In the same vein, the BOD rests heavily on media accounts some of which are nearly two years old—hardly indicating a paramount need for swift action. *See, e.g.*, BOD Information at *Id*. Ex. E at p. 8, n.25 (Fox News); pp. 10-11, n.38, 40, 42 and p. 18, n.59 (Bloomberg).

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 Id*. Ex. D at 4. Rather, 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 draconian. *Id*.

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

The *Mathews* factors weigh in favor of pre-deprivation notice and process consistent with the "fundamental norm" of due process. *See NCRI*, 251 F.3d at 205. In *Ralls*, for example, despite doubts about the second *Mathews* factor (risk of an erroneous deprivation, and the probable value of additional or substitute procedural safeguards) and notwithstanding the government's 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).

Finally, and again, the Court need find only that Plaintiffs are *likely* to succeed on this claim—not that they definitively will. *See also, e.g., Art-Metal—USA, Inc. v. Solomon*, 473 F.

Supp. 1, 4 (D.D.C. 1978) ("With respect to Art Metal's likelihood of success on the merits, it is clear at the outset that due process of law requires that before a contractor may be blacklisted (whether by debarment or suspension) he must be afforded specific procedural safeguards, including, *inter alia*, a notice of the charges against it, an opportunity to rebut those charges and, under most circumstances, a hearing…. Inasmuch as defendants readily concede that Art Metal has been afforded none of these basic protections, plaintiff's chance of succeeding on the merits is extremely high if it has in fact been debarred or suspended.")(citations omitted).

b. 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 therefore was deprived of a meaningful opportunity to rebut it. As explained 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. Fayhee Decl. Ex. L (Ex. 1 thereto). This 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—for example, that under Russian law Kaspersky Lab is considered an "organizer of the dissemination of information on the Internet." Maggs Report at Fayhee Decl. Ex. L (Ex. 1

thereto, ¶ 13(d)). 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., Id*. at pps. 6-8, 16-17. DHS's (initial) Decision and the BOD Information asserted more generalized arguments about Russian law (s*ee id*. Ex. E at 12-14), 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. 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 Id*. Ex. L (Ex. 1 thereto, ¶¶ 1-10 and Appendix 1). This is important, as he draws conclusions based on his own subjective interpretation of Russian law. *See, e.g., Id.* at ¶ 55 ("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 are also likely to 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. *See, generally, e.g., Doe*, 2017 U.S. Dist. LEXIS 178892, at *110 ("The Court's task at this time is to determine whether Plaintiffs have stated *plausible claims and demonstrated a likelihood*—not a certainty—of success based on the present record. The Court is persuaded that Plaintiffs have made these *fairly modest showings*… ")(emphasis added).

B. Plaintiffs are Likely to Show that the BOD is Unsupported by Substantial Evidence and therefore is Arbitrary and Capricious

Under the "arbitrary and capricious" test in 5 U.S.C. § 706(2)(A), the Court must reverse an agency's decision not supported by substantial evidence.[6] *See, e.g., Safe Extensions, Inc. v. FAA*, 509 F.3d 593 (D.C. Cir. 2007).[7] The BOD fails this test 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." Fayhee Decl. Ex. D at 4.

First, as a threshold matter, DHS does not meaningfully rely on agency fact-finding to support this conclusion. Rather, as noted above, DHS's principal and overwhelming source of "evidence" is uncorroborated news reports.[8] In an attempt to satisfy the "substantial evidence" requirement, Defendants characterize these articles and other unsubstantiated allegations as "a

[6] 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). *See also, generally, Poett v. United States*, 657 F. Supp. 2d 230, 242 (D.D.C. 2009)(applying arbitrary and capricious standard to "whether the FBI *reasonably suspected* Plaintiff of having *knowing* involvement with [terrorist organization]"—the "key inquiry" as framed by the definitional requirements of the underlying statute in question)(emphasis in original).

[7] "[T]he arbitrary and capricious test … subsum[es] the substantial evidence test…" *Larkin Chase Nursing & Restorative Ctr. v. Shalala*, 2001 U.S. Dist. LEXIS 23655 (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).

[8] *See BOD Information* at Fayhee Ex. E, citations to: Rachel Madow Show at p. 7, n.5; pps. 10-11, n.37; p. 14, n.50; p. 20, n.66; Fox News at p. 8, n.25; Wired Magazine at p. 9, n.28, 31; p. 10, n.34, 37; p. 12, n.45, 46; p. 18, n.55; Bloomberg at p. 10, n.32, 33; p. 11, n.38, 39, 40, 42; p. 18, n. 59; Forbes at pps. 18-19, n.61.

substantial body of evidence." *Id*. Ex. L at 23. Indeed, as noted above, Manfra testified that she could not "make a judgment off of press reporting."[9]

Manfra publicly testified that the Government *does not have conclusive evidence* that Kaspersky Lab had facilitated any breach of U.S. national security.[10] In addition, DHS confirmed in its Final Decision that it has no evidence of any such breach or wrongdoing on the part of Kaspersky Lab in a section of the Final Decision's Information Memorandum entitled "No Need for Evidence of Wrongdoing." *Id*. Fayhee Ex. L at 9. DHS has roundly ignored its obligation to produce any meaningful and specific evidence against Plaintiffs.

Plaintiffs submit that DHS's findings do not rise to the level of substantial evidence and therefore Plaintiffs have demonstrated a likelihood of succeeding on this claim. *See, e.g., Alf*, 666 F. Supp. 2d at 67 ("As a result, it is likely that the plaintiff will successfully persuade the court that the debarring official failed to articulate a rational connection between the facts found and the choice made.")(internal quotation omitted)

II. Plaintiffs Have Immediately Suffered, and will Continue to Suffer, Irreparable Harm in the Absence of Preliminary Relief.

In order to satisfy the irreparable injury requirement, "[f]irst, the injury must be both certain and great; it must be actual and not theoretical." *Doe*, 2017 U.S. Dist. LEXIS 178892, at *110. "Second, the injury must be beyond remediation." *Id. at* *110 (quoting *Chaplaincy of Full Gospel Churches v. England*, 454 F.3d 290, 297 (D.C. Cir. 2006)). Here, Kaspersky Lab continues to suffer irreparable harm based on the injury to its reputation, and the Company's resulting financial losses.

[9] *See Bolstering the Government's Cybersecurity: A Survey of Compliance with the DHS Directive, supra* at 1:42:41.

[10] *Id*. at 1:24:51.

A. Irreparable Damage to Kaspersky Lab's Reputation.

"[I]t is well-established that reputational injury can be used to establish irreparable harm in certain circumstances." *Toxco Inc. v. Chu*, 724 F. Supp. 2d 16, 30 (D.D.C. 2010)(internal quotation omitted). For example, this Court found a preliminary injunction warranted when a plaintiff demonstrated that he is "rapidly losing the benefit of the business connections [he has] built over the past twenty years, as those connections lose trust in [him] because of the stigma attached with [his] debarment…." *Alf*, 666 F. Supp. at 70.[11]

It is beyond any reasonable dispute that the BOD is causing and will continue to cause profound reputational harm to Kaspersky Lab. As noted above, DHS issued a press release accompanying the BOD on September 13, 2017, which announced 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*

[11] *See also, Atlas Air, Inc. v. Int'l Bd. of Teamsters*, 2017 U.S. Dist. LEXIS 196472, *105 (D.D.C. Nov. 30, 2017)(express cargo shipping airline's "most compelling contention is that …[labor induced slowdown]…would cause the company irreparable reputational harm") (citations omitted); *Patriot, Inc. v. HUD*, 963 F. Supp. 1, 5 (D.D.C. 1997)("plaintiffs have demonstrated irreparable harm in damage to their business reputation," resulting from "HUD's characterization of them …as 'enticing' senior citizens into meetings, and 'pressuring' them to obtain reverse mortgages 'under the guise of sound estate planning.'"); *Nalco Co. v. EPA*, 786 F. Supp. 2d 177, 188 (D.D.C. 2011)(granting preliminary injunction where irreparable injury, in part, was the threatened loss of business "goodwill"); *Reinhard v. Johnson*, 209 F. Supp. 3d 207, 220 (D.D.C. 2016) ("Although 'reputational injury can be used to establish irreparable harm in certain circumstances...as with all other forms of irreparable harm, the showing of reputational harm must be concrete and corroborated, not merely speculative.'")(*quoting Trudeau v. FTC*, 384 F. Supp. 2d 281, 297 (D.D.C. 2005), *aff'd*, 456 F.3d 178 (D.C. Cir. 2006)).

> *reducing potential vulnerabilities, protecting against cyber intrusions, and anticipating future threats.*

Fayhee Decl. Ex. G at 1-2. DHS also published the BOD in the Federal Register on September 19, 2017. (82 Fed. Reg. 43,782, 43,783 (Sept. 19, 2017)(DHS "has determined that the risks presented by Kaspersky-branded products justify issuance of this [BOD].")).

Kaspersky Lab markets itself as a leading *defensive* cyber technology company, focused exclusively on *protecting against* cyberthreats no matter their origin, and so, in accusing the Plaintiffs' products of themselves being a cyberthreat, the BOD caused immediate harm to the Company's reputation and core values. Gentile Decl. at ¶ 15. Thus, the BOD's reputational harm immediately manifested as soon as the BOD was issued—notably on Amazon.com customer reviews. *See Id.* at ¶¶ 16-17; Fayhee Decl. Ex. O. In fact, one of the Amazon customer reviews literally copies and pastes portions of the DHS press release excerpted immediately above. Fayhee Decl. Ex. O, at p. 1 (see review by "Aircarl on September 13, 2017"- "*DHS gives agencies 90 days to remove Kaspersky Lab IT from Networks*").

Preliminary rescission of the BOD would qualitatively change Kaspersky Lab's standing in the market. The Company naturally will be on stronger ground in addressing immediate customer concerns should the BOD be preliminarily rescinded. Gentile Decl. at ¶ 24. Currently, 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. See generally, e.g., KindHearts for Charitable Humanitarian Dev., Inc. v. Geithner*, 676 F. Supp. 2d 649, 654 (N.D. Ohio 2009)("Although defendants have already denominated [plaintiff] as 'under investigation' for possible designation as an SDGT [Specially Designated Global Terrorist], the damage to [plaintiff]'s reputation and donor goodwill attending actual designation differs qualitatively from, and would be far greater than, the stigma associated with being under investigation. This is akin

to the difference between recovering from being under criminal investigation and recovering from a criminal conviction.")(establishing irreparable injury on reputational harm). Plaintiffs remain willing and able to work with DHS to address any legitimate concerns that it has regarding Kaspersky Lab software, or that of similarly situated vendors. Gentile Decl. at ¶ 27.

B. The BOD has Caused Kaspersky Lab to Suffer Substantial Financial Losses

In APA cases such as this, financial harm *cannot* be recovered from the government and is therefore necessarily irreparable. This Court has consistently found such unrecoverable financial harm supports preliminary injunctive relief—and this matter warrants a similar result. For example, in *Feinerman v. Bernardi*, 558 F. Supp. 2d 36, 51 (D.D.C. 2008), involving debarment instituted by the Department of Housing and Urban Development, this Court granted a preliminary injunction on an APA claim, explaining that while as a "general matter" monetary loss is not irreparable unless it presents an existential threat to a business, "where, as here, the plaintiff … cannot recover damages… due to the defendant's sovereign immunity, any loss of income suffered by a plaintiff is irreparable *per se*." *See also*, *Alf* , 666 F. Supp. 2d at 70 (granting preliminary injunction against enforcement of debarment, reasoning that "by virtue of the government's sovereign immunity, the plaintiff will be unable to recoup his lost income if he remains unable to obtain other government contracts.")(*citing Feinerman*, 558 F. Supp. 2d at 51) *Smoking Everywhere Inc. v. FDA*, 680 F. Supp. 2d 62 (D.D.C. 2010)(granting preliminary injunction on APA claim, and noting that "even if the claimed economic injury did not threaten plaintiffs' viability, it is still irreparable because plaintiffs cannot recover money damages against FDA.")(citations omitted); *Nalco Co. v. EPA*, 786 F. Supp. 2d 177, 188 (D.D.C. 2011)(granting preliminary injunction on APA claims, on the ground that "EPA's actions threaten a loss of sales and goodwill for which [plaintiff] will have no right of recourse against

the federal government.")(*citing Feinerman*, 558 F. Supp. 2d at 50-51)*; see also, e.g., Children's Hosp. of the King's Daughters, Inc. v. Price*, 258 F. Supp. 3d 672, 690 (E.D. Va. 2017)(granting preliminary injunction on APA claims, finding irreparable injury because "'any loss of income suffered by a plaintiff is irreparable *per se*.'")(*quoting Feinerman*, 558 F. Supp. 2d at 51).

In other decisions, this Court has made clear that insignificant unrecoverable losses will not establish irreparable harm pursuant to this theory. For example, in *Air Transport Ass'n of America v. Export-Import Bank*, this Court explained:

> [The irreparable *per se*] argument stretches too far. Any movant that could show any damages against an agency with sovereign immunity—even as little as $1—would satisfy the standard. The wiser formula requires that the economic harm be *significant*, even where it is irretrievable because a defendant has sovereign immunity….[Thus,] [w]here a movant makes a strong showing that the economic loss would significantly damage its business above and beyond a simple diminution in profits…irreparable harm may be established.

840 F. Supp. 2d 327, 335-336 (D.D.C. 2013) (internal quotation omitted)(emphasis added). But this makes little difference here because Kaspersky Lab's losses resulting from the BOD are clearly significant—and in fact, the financial impact is continuing and growing. Gentile Decl. ¶ 19. As set forth in the Facts (Section IV), *supra*, following the issuance of the BOD, several U.S. retailers removed Kaspersky Lab products from their shelves and suspended their long-standing partnerships with the Company. *Id. at* ¶ 20. Several of these retailers, which have provided a steady stream of both new customers and consumer product subscription renewals to Kaspersky Lab over the years, encouraged and incentivized existing Kaspersky Lab software customers (current license holders) to "switch" to the software of Kaspersky Lab's competitors—following removal of Kaspersky Lab products from their shelves and online offerings. *Id.*

The result was an immediate 37% and 61 % fall in Kaspersky Lab Inc.'s 2017 Q3 and Q4 gross bookings from U.S. retail sales, respectively, compared to the same period in 2016.[12] *Id*. at ¶¶ 20, 21. And the company's gross bookings from U.S. retail sales in the second half of 2017 fell 50%, compared to the same period in 2016. *Id*. at ¶ 21.

As noted earlier, in addition to the decline in the consumer market, Kaspersky Lab, Inc.'s 2017 business-to-business sales fell 33% in Q3 and 45% in Q4 when compared to the same period in 2016. *Id*. at ¶ 22. The license renewal rate of existing B2B customers fell 23 percentage points in the second half of 2017 compared to the same period in 2016. *Id*.

Customers have terminated several substantial tenders for Kaspersky Lab products that were in process at the time of the BOD as a result of its issuance and in many cases before the Final Decision was issued. *Id. at* ¶ 23. The potential B2B customers in these cases have 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*.

An unprecedented volume of product return and early termination requests is also affecting the Company—and in light of the BOD accusations, the Company is accepting returns that it otherwise would have rejected under its standard return policy. *Id. at* ¶ 24. Many customers returning the software for a refund specifically cite the BOD. *Id.* Net loss attributable to product returns to Kaspersky Lab, Inc. from U.S. customers for the period September-December 2017 increased nearly 2300% relative to the same period in 2016 (~$238k versus ~$10k, respectively). *Id.*

Finally, the reputational and financial injury from the BOD is manifesting itself in a substantial headcount reduction at Kaspersky Lab, Inc., from 281 employees in the U.S. on

[12] As noted *supra*, Kaspersky Lab closed and finalized its financial books for Fiscal Year 2017 on January 17, 2018—the day of the filing of this Application. *See* Gentile Decl. ¶19.

September 12, 2017 (the day before the BOD was issued) to 253 employees on January 17, 2018—a 10% reduction in headcount. *Id. at* ¶ 26. This is largely attributable to: i) voluntary departures from the company caused by a fall in staff morale due to the attacks on the reputation and integrity of the company and its products (including through the BOD and statements made by DHS officials); and ii) layoffs necessitated by falling revenues—the Company was forced to lay-off 24 employees in the past month alone. *Id.*

In short, in addition to the reputational harm, Kaspersky Lab's commercial business suffered great, immediate, and certain economic losses that are unrecoverable, due to the BOD. Plaintiffs have made a clear showing of a likelihood of irreparable harm.

III. Balance of Harms and the Public Interest Weigh in Plaintiffs' Favor

Finally, the balance of harms and the public interest, which merge into one factor in this case, also weigh in favor of a preliminary injunction. DHS's argument that the BOD is necessary to protect national security carries little weight because DHS has acknowledged that the Government *does not have conclusive evidence* that Kaspersky Lab has facilitated the breach of any U.S. Government information system, and rather has acted hastily against the company based on uncorroborated allegations contained in years-old news articles. As established above, the BOD simply is not backed by substantial evidence.

Further, the due process violation here also tips this factor, because "it is always in the public interest to prevent the violation of a party's constitutional rights." *Klayman v. Obama*, 957 F. Supp. 2d 1, 42 (D.D.C. 2013), *rev'd on other grounds*, 800 F.3d 559 (D.C. Cir. 2015) (internal quotation omitted). *See also*, *Ass'n of Cmty. Orgs. for Reform Now v. FEMA*, 463 F. Supp. 2d 26, 36 (D.D.C. 2006)("[T]he public has an interest in the government maintaining procedures that comply with constitutional requirements.") (citation omitted); *Olympic Fed. S&L*

v. Office of Thrift Supervision, 732 F. Supp. 1183, 1202-03 (D.D.C. 1990)("[T]he clear violation of plaintiff's constitutional rights and the public's interest in protecting the Constitution outweigh … harms to the public interest."). Thus, for example, in ***KindHearts for Charitable Humanitarian Dev., Inc.***, 676 F. Supp. 2d 649, 655 (N.D. Ohio 2009), the Court entered a preliminary injunction against the designation of plaintiff as a terrorist organization, finding that the constitutional due process violation supported this factor: "The public…has a fundamental and great interest in seeing the Constitution upheld and ensuring that remedies be provided when the government has acted in derogation of constitutional rights." (*citing G & V Lounge v. Mich. Liquor Control Comm.*, 23 F.3d 1071, 1079 (6th Cir. 1994) ("[I]t is always in the public interest to prevent the violation of a party's constitutional rights.")). Accordingly, the constitutional due process violation in this case likewise supports this final factor, and tilts in favor of granting the application.

CONCLUSION

Plaintiffs have shown a strong likelihood of success on the merits, immediate and significant irreparable harm, and have demonstrated that the balance of equities and public interest tips in their favor. Plaintiffs therefore respectfully request that the Court grant their Application, and preliminarily invalidate and rescind the BOD and the December 6, 2017, Final Decision maintaining the BOD, and preliminarily enjoin DHS from enforcing the BOD and the Final Decision.

Dated: January 17, 2018

Respectfully submitted,

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