UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

KASPERSKY LAB, INC. 500 Unicorn Park, 3rd Floor Woburn, Massachusetts 01801; and KASPERSKY LABS LIMITED New Bridge Street House 30-34 New Bridge Street London, EC4V 6BJ United Kingdom Plaintiffs, v. U.S. DEPARTMENT OF HOMELAND SECURITY Washington, D.C. 20528; and Kirstjen Nielsen, in her official capacity as Secretary of Homeland Security Washington, D.C. 20528 Defendants.	)	Civil Action No. _____

COMPLAINT

1. Kaspersky Lab, Inc., a Massachusetts corporation, together with its U.K. parent company Kaspersky Labs Limited ("Plaintiffs" or "Kaspersky Lab"), bring this action under the Administrative Procedure Act ("APA") to uphold their constitutional due process and other rights which Defendants violated through unprecedented, sweeping, and retroactive debarment of Kaspersky Lab from U.S. Government information systems by way of the Department of Homeland Security's ("DHS") Binding Operational Directive 17-01 issued on September 13, 2017 (the "BOD").

2. Without affording Plaintiffs notice or a prior opportunity to be heard, and without sufficient evidence, Defendants branded Kaspersky Lab's market-leading anti-virus products an information security "threat, vulnerability and risk" to U.S. Government information systems and summarily ordered their identification, removal, and discontinuation by all subject U.S. government agencies, and the private contractors operating within their IT systems.

3. DHS was required under the APA and the U.S. Constitution to afford Plaintiffs due process—at the very least notice and a meaningful opportunity to be heard—*before* debarring Plaintiffs and depriving them of their liberty interest.

4. Defendants never claimed—and nothing in the record suggests—any justification for denying Plaintiffs the basic right to notice and an opportunity to contest Defendants' "evidence" (in substantial part consisting of uncorroborated news articles) *before* the debarment. In particular, DHS has never claimed, and nothing in the records suggests, that the "information security risks" allegedly presented by Plaintiffs' products were so imminent, so exigent, or so urgent, that they would justify depriving Plaintiffs of their constitutional due process rights.

5. Defendants had ample time and opportunity to afford Plaintiffs the due process to which they were entitled prior to the issuance of the BOD, and actively misled Plaintiffs regarding the status of their pre-BOD deliberations. Plaintiffs wrote in good faith to Defendants in July 2017 to offer to discuss and respond to any concerns that Defendants might have regarding Kaspersky Lab products. Defendants replied in August 2017, indicating that they "appreciate[d] [Plaintiffs'] offer to provide information" and would "be in touch again shortly." Instead, Defendants proceeded with issuing the BOD in September, without any prior notice to Plaintiffs or any opportunity for them to be heard.

6. DHS issued the BOD pursuant to the Federal Information Security Modernization Act of 2014, 44 U.S.C. § 3551 *et seq*. (2014) ("FISMA"), which 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." 44 U.S.C.§ 3552(b)(1).

7. The BOD compelled all federal agencies to: (1) identify Kaspersky Lab-branded products on all federal informational systems within 30 days, (2) develop a detailed plan to remove and discontinue the present and future use of all Kaspersky Lab-branded products within 60 days, and (3) unless directed otherwise by DHS based on new information, start actual removal within 90 days. (BOD at 2-3)

8. While DHS professed to give Plaintiffs an opportunity to contest the BOD and change DHS's decision before the 90-day mark, by allowing Kaspersky to make a written submission to DHS near in time to the 60-day mark, this process was illusory and wholly inadequate because it failed to satisfy even the minimum standards of due process.

9. In actuality, the debarment of Plaintiffs and the damage caused was immediate and complete *upon the issuance* of the BOD. The process for identification, removal, and discontinuation had been initiated immediately upon issuance, all government agencies were prejudiced against Plaintiffs' software at that time, and the process could therefore not have been adequately unwound.

10. DHS expressly acknowledged that following its issuance of the BOD, some "agencies removed the software in advance of the BOD's requirement to start removal on day 90" without regard to the purported process set forth in the BOD (*See* Jeannette Manfra, testimony before the House Committee on Science, Space, and Technology, November 14, 2017).

Following the Final Decision, the Department confirmed that, rather than treating the 90 day-mark as the start of the removal process (absent any change to the BOD by Defendants due to submissions received from Plaintiffs or other affected parties), many agencies had actually removed the software by that time: "For the most part, we're closed out on removing the Kaspersky [antivirus]-branded products." (*See* Christopher Krebs press briefing, December 13, 2017).

11. Plaintiffs submitted a detailed written response to the BOD on November 10, 2017 (the "Kaspersky Lab Submission").

12. DHS issued a Final Decision on December 6, 2017.

13. Having already committed themselves, and their subject agencies, to detrimental action against Plaintiffs, Defendants failed to adequately consider, or respond to, the Kaspersky Lab Submission. Defendants simply re-asserted the BOD un-amended through the Final Decision.

14. Even in their Final Decision and supporting materials, Defendants continued to introduce new allegations, facts, and legal arguments to which Plaintiffs have had no opportunity to respond, even pursuant to the professed (but inadequate) administrative process advanced by Defendants which concluded with the Final Decision.

15. Accordingly, Plaintiffs were harmed before any due process was offered at all, and were never granted any meaningful process by which to challenge the administrative action in the BOD prior to the debarment. The debarment therefore deprived Kaspersky of a constitutionally protected liberty interest without due process of law, in violation of the Fifth Amendment of the Constitution.

16. The BOD also fails to meet the evidentiary requirements of the APA. Instead of relying on agency fact-finding, DHS's principal and overwhelming source of "evidence" is uncorroborated news reports (some citing anonymous sources)—including the Rachel Maddow Show, Fox News, Wired Magazine, Bloomberg News, and Forbes.

17. In an attempt to satisfy the APA's "substantial evidence" requirement, Defendants have mis-categorized these articles and other unsubstantiated allegations as "a substantial body of evidence." (Final Decision Information Memorandum at 23).

18. To the contrary, Jeannette Manfra, the DHS author of the Information 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 fact the Government *does not have conclusive evidence* that Kaspersky Lab had facilitated the breach of any U.S. Government information system. When asked in the same hearing by the Committee Chairman to address other media reports regarding Plaintiffs, Manfra testified that she could not "make a judgement based off of press reporting." Yet that is exactly what she asked DHS's Acting Secretary to do in her memoranda in support of the BOD and the Final Decision.

19. DHS confirmed in its Final Decision that it has no evidence of any such breach or wrongdoing on the part of Kaspersky Lab in an entire section of the Final Decision's Information Memorandum entitled "No Need for Evidence of Wrongdoing." DHS roundly ignores its obligation to produce any meaningful and specific evidence against Plaintiffs.

20. For these reasons, Plaintiffs bring this suit challenging the BOD and the Final Decision under the APA, as violative of Plaintiffs' Fifth Amendment right to due process, and as arbitrary and capricious and not based on substantial evidence. Plaintiffs seek declaratory relief

that the BOD and Final Decision are invalid, and preliminary and permanent injunctive relief to rescind them and enjoin enforcement.

PARTIES

21. Plaintiff Kaspersky Lab, Inc. is a Massachusetts corporation with its principal place of business in Woburn, Massachusetts. Plaintiff Kaspersky Lab, Inc. is a directly wholly-owned subsidiary of Plaintiff Kaspersky Labs Limited, a U.K. holding company.

22. Defendant DHS is the federal agency responsible for issuing and implementing the BOD and Final Decision at issue in this case.

23. Defendant Kirstjen Nielsen is the Secretary of DHS and is being sued in her official capacity only.

JURISDICTION AND VENUE

24. This action arises under the Due Process clause of the Fifth Amendment of the Constitution and the APA, 5 U.S.C. §§ 500-596, 701 *et seq*. This Court has jurisdiction pursuant to 28 U.S.C. §§ 1331 and the APA.

25. The Court has the authority to grant declaratory and injunctive relief pursuant to 28 U.S.C. §§ 2201 and 2202, and its inherent equitable powers.

26. Venue is proper in this district pursuant to 28 U.S.C. § 1391(e)(1).

FACTUAL ALLEGATIONS

I. Kaspersky Lab, Its Reputation in the Industry, and Its Principles of Fighting Cyberthreats

27. Kaspersky Lab is a multinational cybersecurity company exclusively focused on protecting against cyberthreats, no matter their origin. It is one of the world's largest privately owned cybersecurity companies. It operates in 200 countries and territories and maintains 35

offices in 31 countries. Among its offices are research and development centers employing anti-malware experts in the U.S., Europe, Japan, Israel, China, Russia, and Latin America.

28. Although the corporate group's global headquarters are in Moscow, more than 85% of Kaspersky Lab's sales are generated outside of Russia. 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.

29. 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.

30. Kaspersky products have received top ratings for malware detection (among other performance factors). For example, in 2016, Kaspersky Lab products participated in 78 independent tests & reviews—and the company was awarded 55 first places and 70 top-three finishes. Kaspersky Lab consistently ranks among the world's top four vendors of security solutions for endpoint users.

II. Kaspersky Lab, Inc. and Sales to the U.S. Government

31. Founded in 2004, Kaspersky Lab, Inc. is a Massachusetts corporation and is a directly wholly-owned subsidiary of Kaspersky Labs Limited. Kaspersky Lab, Inc. acts as the company's North American headquarters through offices in Woburn, Massachusetts and employs nearly 300 people in the U.S.

32. The U.S. has been and remains one of the most significant geographic markets in Kaspersky Lab's global business. Sales to customers in the United States represent approximately one quarter of total global bookings in 2016. Plaintiff Kaspersky Lab, Inc. has

invested over half a billion dollars in its operations over the last twelve years, and over $65 million in 2016 alone.

33. Active licenses held by federal agencies have a total value (to Plaintiffs) of less than USD $54,000, which represents a tiny fraction (0.03%) of Plaintiff Kaspersky Lab, Inc.'s annual sales in the United States.[1]

34. Notwithstanding the limited volume of U.S. Government sales, Kaspersky Lab, Inc. has a substantial interest in its status as a vendor to the U.S. Government, and in its continued ability to sell its product to the U.S. Government, inclusive of the right to be free of disparagement prejudicing commercial and enterprise customers.

III. Without Affording Plaintiffs Notice or Opportunity to Be Heard, DHS Issued an Immediate and Complete Ban of Kaspersky Lab from all Government Agencies

35. On September 13, 2017, without affording any notice to Kaspersky Lab or prior opportunity to rebut the allegations, and despite Plaintiffs' July 2017 outreach and Defendants' professed willingness to enter into discussion in August, DHS announced that it had "determined that the risks presented by Kaspersky-branded products justify the issuance of" Binding Operational Directive 17-01 ("**Removal of Kaspersky-Branded Products**"). (BOD at 1). The BOD, as explained below, effectively banned all U.S. government agencies from using Kaspersky products and debarred the company immediately. Additionally, it required existing software instances to be identified and removed. The BOD applied to virtually all products, solutions, and services supplied, directly or indirectly, by Kaspersky Lab.[2] (*Id*. at 2). In the accompanying Decision, DHS branded Kaspersky Lab products a threat to U.S. national security,

[1] Based on Plaintiff Kaspersky Lab, Inc.'s 2016 net booking data.
[2] The BOD excepted two specific services, Kaspersky Threat Intelligence and Kaspersky Security Training. (BOD at 2).

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." (Decision at 2).

36. DHS issued the BOD pursuant to FISMA, which 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*. at 1, *citing* 44 U.S.C.§ 3552(b)(1)).

37. Specifically, DHS claimed that FISMA justified the BOD because "unclassified evidence"—almost entirely uncorroborated media reports, several citing anonymous sources—established that "[a]s 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." (Decision at 2).

38. The BOD compelled all federal agencies to: (1) identify the use or presence of Kaspersky Lab-branded products on all federal informational systems within 30 days, (2) develop a detailed plan to remove and discontinue present and future use of all Kaspersky Lab-branded products within 60 days, and (3) start the actual removal within 90 days, unless directed otherwise by DHS in light of new information obtained by DHS, including but not limited to new information submitted by Kaspersky. (the "30-60-90 day structure") (BOD at 2-3). 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.

IV. The BOD's Purported Administrative Process

39. In a separate letter to Plaintiffs accompanying the BOD, DHS claimed to Plaintiffs that it was providing an "administrative process to inform [DHS] decision making"—a process to be later set forth in a Federal Register Notice—but as explained below, that process had no bearing on the debarment already effectuated by the BOD, and was purely perfunctory. (*See* DHS Letter to Eugene Kaspersky, dated September 13, 2017).

40. On September 19, 2017, DHS did indeed announce 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. 180, 43783, 43784 (Sept. 19, 2017)). DHS gave Plaintiffs until November 3, 2017 (subsequently extended to November 10, 2017) to respond to the BOD.

41. The Federal Register further provided that, following DHS's receipt of a response to the BOD, "…the Secretary's decision will be communicated to the entity in writing by December 13, 2017." (*Id.*) But this was one day *after* the 90-day deadline by which agencies were to have begun removing Kaspersky products. In apparent acknowledgement of this procedural deficiency, the Information Memorandum accompanying the Final Decision "recommend[s] 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. (Final Decision Information Memorandum at 3).

42. On September 29, 2017, DHS retrospectively provided Plaintiffs, through their counsel, access to an internal 21-page DHS Information Memorandum drafted and submitted to

the then Acting DHS Secretary on September 1, 2017, in support of the BOD (the "BOD Information").

43. On November 10, 2017, Plaintiffs delivered to the Defendants the Kaspersky Lab Submission, an extensive written response to the BOD and its Information.

44. The Kaspersky Lab Submission rebutted at length the legal and factual allegations levied against Plaintiffs, corrected many misunderstandings held by DHS (as perpetuated by the news articles it cited), and highlighted the deficiencies in the administrative process offered by Defendants.

45. Following the issuance of the BOD, DHS had repeatedly declined the requests of Plaintiffs and their counsel to engage in order to present the Company's position, address DHS's concerns, and discuss any potential options for mitigation. Following the Kaspersky Lab Submission, DHS did finally agree to meet with Plaintiffs' representatives and counsel on November 29, 2017. At that meeting Plaintiffs responded to a number of questions from Defendants' attorneys regarding the Kaspersky Lab Submission but Defendants did not offer any further support for the BOD, much less an indication that they were willing to rectify the procedural or substantive deficiencies in the BOD or consider any mitigating options short of the outright ban contemplated by the BOD.

46. Plaintiffs believe that such options were available to Defendants and have not been fully explored, either prior to or subsequent to the issuance of the BOD.

47. On December 6, 2017, and without any adequate consideration of the Kaspersky Lab Submission, DHS issued a "Final Decision maintaining BOD 17-01 without modification" (the "Final Decision"). The Final Decision was accompanied by a Letter to Plaintiffs and an

Information Memorandum directed to the Acting Secretary in support of the Final Decision (the "Final Information").

V. Without Justification, Defendants' Administrative Process Provided No Notice or Opportunity to be Heard Prior to Deprivation

48. Although the BOD's 30-60-90 day structure gives the impression that harm is not immediate, in reality, the BOD is an immediate and complete debarment of Kaspersky Lab from government business upon issuance.

49. 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"), Jeanette Manfra, DHS Assistant Secretary for Cybersecurity and Communications, 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." 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. Thus, federal agencies had begun removing Kaspersky software long before DHS even had completed its review of the Kaspersky Lab Submission.

50. The BOD, supported by other actions in Congress, has also had a severe adverse impact on Kaspersky's other commercial interests in the U.S., which begun long before the Defendants' decision was officially declared "Final." For example, several retailers have

removed Kaspersky Lab products from their shelves and suspended their long-standing partnerships with Kaspersky Lab following the issuance of the BOD. As a result of these and other actions, Plaintiffs' 2017 Q3 retail sales have fallen significantly compared to the same period in 2016. Presently, Plaintiffs are receiving and processing an unprecedented volume of product return and early termination requests as a result of DHS and other U.S. Government actions, which customers specifically refer to when stating the reason for their return.

51. Indeed, Christopher Krebs, the Senior Official Performing the Duties of the Under Secretary for the National Protection and Programs Directorate, who participated in the recommendation that the BOD be issued, stated DHS's intent bluntly during public statements on October 31 2017: "[W]hen [DHS] makes a pretty bold statement like issuing the Kaspersky Lab binding operational directive I think that's a fairly strong signal [to consumers]."[3] This statement was made in response to a question regarding how and to what extent consumers should be informed as to the nature of any risk posed by Kaspersky Lab products in light of the recent issuance of the BOD. The fact that a senior DHS official decided to make a statement of that nature at the same time Defendants were purporting to offer Kaspersky Lab a genuine and meaningful right to be heard makes clear that the DHS specifically intended to prejudice Kaspersky Lab's commercial interests even before the expiration of DHS's own arbitrarily imposed process and deadline for the implementation of the BOD.

52. Krebs also confirmed through his statements to the media following the Final Decision that, with his oversight, federal agencies had actually been removing Kaspersky Lab-branded software, while this process was purported to be running, prior to the 90-day mark.

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

53. Kaspersky had no opportunity to test or rebut the "evidence" contained in the BOD or its Information *before* action was taken (at the time the BOD was issued), and therefore there has been no *opportunity to effectively be heard*.

54. Rather, under the circumstances, the Fifth Amendment required DHS to provide Plaintiffs procedural protections *before* debarring it through the BOD. Critically, DHS made no attempt to demonstrate how prior notice to Plaintiffs would have interfered with DHS's goals of eliminating the alleged "information risks." Nor did DHS show why it failed to consider less severe measures or potential mitigation that could have been imposed on Kaspersky to address DHS's purported concerns. DHS's failure to provide adequate and timely notice created a substantial risk of wrongful deprivation.

55. As explained above, the BOD, the Decision, its Information, the Final Decision, and the Final Information are all devoid of even a suggestion that the "information security risks" allegedly presented by Kaspersky Lab are imminent, exigent, or urgent—let alone to a degree that justify foreclosing pre-deprivation notice.

56. To the contrary, DHS provides *three months* for affected agencies to "begin to implement their plan of action." (BOD at 2). 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 8 n.23, 10 n.38.)

57. 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 Federal Acquisition Regulations ("FAR"). 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: unlike a debarment pursuant to the FAR, the BOD is prospective as well as

retrospective, requires the removal of Kaspersky-branded products "indefinitely," and prevents third parties from selling products produced by Kaspersky. (Decision at 4). And so, paradoxically, even though it is more thorough in depriving Kaspersky Lab of its rights, the BOD provides far less adequate process than the FAR, which has a well-established and constitutionally adequate due process that requires agency decisions be made in consideration of a contractor's response before any action is taken to exclude it from future government contracts.

58. Defendants, in fact, had ample opportunity to provide Kaspersky Lab with due process protections prior to the issuance of the BOD. Unaware of what action, if any, DHS was contemplating, Kaspersky Lab wrote to DHS on July 18, 2017, with an offer to provide any information or assistance with regard to any investigation involving the Company, its operations, or its products. 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." Nearly one month later, and absent any other communication from DHS, the BOD was issued.

VI. DHS's Introduction of New Evidence in its Final Decision also Violates Due Process

59. Aside from failing to provide due process prior to the issuance of the BOD, the process which DHS professed to provide Plaintiffs after its issuance was not meaningful or fair.

60. DHS based the BOD at least in part on a supposed concern about Russian law. In its December 6, 2017, Final Decision, DHS 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')." (Final Decision at 2).

61. Rather than introducing the Maggs Report with the September 13, 2017, BOD—which would have enabled Plaintiffs to address the report when Plaintiffs filed the Kaspersky Lab Submission—DHS withheld (or did not obtain) the report until its December 6, 2017, Final

Decision. This approach denied Plaintiffs basic due process by unfairly foreclosing Plaintiffs any opportunity to rebut or contest the Maggs Report.

VII. The BOD is Based Almost Entirely on Uncorroborated Media Reports—Not Substantial Evidence—and therefore is Arbitrary and Capricious

62. The BOD and the Final Decision are based on the following three broad allegations levied against Plaintiffs and their software:

> [1] the broad access to files and elevated privileges of anti-virus software, including Kaspersky software; [2] ties between Kaspersky officials and Russian government agencies; and [3] requirements under Russian law that allow Russian intelligence agencies to request or compel assistance from Kaspersky and to intercept communications transiting between Kaspersky operations in Russia and Kaspersky customers, including U.S. government customers.
>
> (Final Decision, p. 2-3)

63. DHS's record underlying the BOD in support of these three arguments is devoid of reliable evidence. Rather, the BOD is based on a series of uncorroborated news articles, most of which rely upon the same anonymous sources, none of which have been tested in a fair and public forum.

A. Broad access to files and elevated privileges of anti-virus software, including Kaspersky Lab software

64. DHS relies on an assumption that a particular software product or vendor should be banned because of a generally presumed susceptibility to exploitation by a malicious actor, but, tellingly, it does not extend such a prohibition to other software products beyond anti-virus software or to other anti-virus software vendors besides Kaspersky Lab.

65. Kaspersky Lab software operates in a manner that closely mirrors the offerings of other providers which have not been subject to the DHS action. Neither the BOD Information, nor the assessment by the National Cybersecurity and Communications Integration Center

("NCCIC Assessment") on which it relies, provide any technical evidence to indicate that any Kaspersky Lab product represents either a greater or lesser technical risk to federal information systems than similar anti-virus software products or vendors.

66. As noted above, Kaspersky Lab's U.S. government business represents a small fraction of its U.S., much less its global, business and software footprint. Other anti-virus software products have a much larger footprint across federal government systems and are likely as vulnerable to exploitation by malicious cyber actors as DHS alleges is the case for Kaspersky-branded software products.

67. Thus, if DHS's claims about anti-virus software were legitimate, DHS would apply the BOD to other software rather than to Kaspersky Lab products alone.

B. Ties between Kaspersky Lab and the Russian government

68. There is no evidence presented by DHS of improper coordination between Kaspersky Lab or its executives and the Russian Government in furtherance of demonstrable illicit activities. Rather, DHS speculates that cybersecurity risks are presented by Kaspersky Lab products merely by virtue of the fact that the Company is headquartered in Moscow.

69. DHS's stated concern that the Russian Government engages in cyberespionage (*see, e.g.*, Decision at 2) is not evidence that any global company like Kaspersky Lab headquartered (or with operations) in Russia, are facilitating government sponsored cyber-intrusions.

70. In fact, more than 85 percent of Kaspersky Lab's revenue comes from outside of Russia—a powerful economic incentive to avoid any action that would endanger the trusted relationships and integrity that serve as the foundation of its business by conducting inappropriate or unethical activities with any organization or country.

71. The BOD Information further alleges that Kaspersky Lab senior executives have "ties" with the Russian government and highlights, among other things, their long ago former service within the Russian government and/or military and their current profiles and connections. (BOD Information at 10-11). It fails to acknowledge, however, that each of these individuals grew up in the Soviet Union at a time when the government relied heavily on conscripted service. As such, allegations of this sort could be made against the majority of Russians of the same generation. These facts do not indicate that their connections or service with the Russian Government were, or are, inappropriate or that they have continued to this day.

72. Moreover, DHS does not suggest that an inappropriate relationship (between Kaspersky Lab and the Russian Government or otherwise) is likely or probable—or even that there is *any* relationship whatsoever. DHS simply suggests that such an inappropriate relationship is *possible:* "Such an established relationship and connections between Kaspersky and the FSB [(Russian Security Services)] could facilitate future cooperation for other purposes and therefore is an area of serious concern to DHS." (Final Information at 13)(emphasis added).

C. Requirements under Russian law

73. The BOD Information alleges that Kaspersky Lab has obtained certificates and licenses from the Russian Security Services ("FSB"), and that this "suggest[s] an unusually close" relationship between the two. (BOD Information at 9). But there is simply nothing unusual about the licenses or certificates Kaspersky Lab has obtained from the FSB in the normal course of doing business in Russia. All information technology companies involved in cryptography-related activities operating in Russia (including leading U.S. companies) are required to obtain the same licenses and certificates from the FSB. In recognizing this exact role of the FSB in granting certificates for certain commercial products, the U.S. Department of the

Treasury's Office of Foreign Assets Control issued General License No. 1 under the Cyber Sanctions Executive Orders which expressly authorized U.S. companies to obtain precisely the same licenses from the FSB in a way that would otherwise have been prohibited due to the FSB's prior designation under those sanctions authorities.

74. DHS also claims that the BOD is warranted based on the FSB's authority to compel or request assistance from companies in Russia. (Decision at 2; BOD Information at 2, 12). However, this obligation applies to all companies operating in Russia. The FSB can request information from companies in Russia only in furtherance of specified duties—and are subject to challenge in Court. Defendants fail to provide any evidence of the FSB actually compelling Plaintiffs to provide any information on Plaintiffs' customers in the U.S. or any other evidence of Plaintiffs' interaction with Russian authorities that would pose a security threat to federal agencies using the software in the U.S.

VIII. Defendants' Failure to Acknowledge and Fulfill Due Process and APA Protections

75. DHS, through its actions and statements described above, has demonstrated its willing failure to comply with the requirements of the APA and the U.S. Constitution in issuing the BOD. Plaintiffs explained these violations in the Kaspersky Lab Submission.

76. Rather than responding to these deficiencies and attempting in any way to remedy them, DHS cursorily dismissed them in its Final Decision and Information. DHS says simply that it is: "confident that the BOD procedures are constitutional and lawful," that the "BOD is based on a substantial body of evidence," and that DHS "provided Kaspersky with meaningful notice and opportunity to confront the evidence against it." (Final Information at 23.)

77. For the reasons set out in this Complaint, this is not the case. DHS has not, in the Final Information, the Final Decision, or anywhere else, demonstrated its fulfillment of its obligations under the APA or the U.S. Constitution.

EXHAUSTION, FINALITY, AND STANDING

78. Plaintiffs have exhausted the professed "administrative process" provided by DHS as described above, through the November 10, 2017, Kaspersky Lab Submission.

79. Plaintiffs challenge a "final agency action" for purposes section 704 of the APA. After DHS issued the BOD, and Plaintiffs submitted the Kaspersky Lab Submission, DHS issued its "Final Decision maintaining BOD 17-01," as explained above.

80. Plaintiff Kaspersky Lab, Inc. has standing to bring this suit because the Company sold its products (through its partners) to the U.S. Government, and is injured by the debarment effectuated by the BOD. The company also has been injured by DHS's disparagement of the Company through the BOD.

81. Plaintiff Kaspersky Labs Limited also has standing. As the U.K. parent, Kaspersky Labs Limited suffers financial harm due to its wholly-owned subsidiary's loss of sales and reputational injury, resulting from the BOD. Kaspersky Labs Limited is also injured by the BOD's preclusive effect. The BOD orders all federal agencies to discontinue all Kaspersky-branded software, thereby precluding Kaspersky Labs Limited from making a direct sale to the U.S. Government.

FIRST CAUSE OF ACTION

(Administrative Procedure Act, 5 U.S.C. § 706(2)(B) and the Due Process Clause of the Fifth Amendment of the United States Constitution)

82. Plaintiffs incorporate by reference, as if fully restated herein, paragraphs 1-81 above.

83. The APA directs that the "the reviewing court shall ... hold unlawful and set aside agency actions, findings, and conclusions found to be … contrary to constitutional right, power, privilege, or immunity." 5 U.S.C. § 706(2)(B).

84. The BOD, as issued to Kaspersky Lab, and upheld by the Final Decision is unlawful and contrary to constitutional right, power, privilege, and immunity.

85. DHS violated Plaintiffs' Fifth Amendment rights to due process by depriving Plaintiffs of a protected liberty interest, with constitutionally insufficient procedures attendant upon that deprivation. Through the BOD, DHS debarred Plaintiffs from government contracting, and effectively terminated Kaspersky Lab as a government contractor while simultaneously broadcasting to the world insufficient and uncorroborated reasons for that termination. As explained above, DHS was required to provide pre-deprivation due process, and did not.

SECOND CAUSE OF ACTION

(Administrative Procedure Act, 5 U.S.C. § 706(2)(A))

86. Plaintiffs incorporate by reference, as if fully restated herein, paragraphs 1-81 above.

87. The APA directs that "the reviewing court shall...hold unlawful and set aside agency actions, findings, and conclusions found to be…arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. § 706(2)(A).

88. The BOD is not supported by substantial evidence. DHS did not properly evaluate the strength of the evidence before it, and therefore failed to satisfactorily support its decision or identify a rational connection between the facts before it and the conclusions it reached. Accordingly, the BOD was arbitrary and capricious and an abuse of agency discretion.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that a judgment be granted:

(a) Preliminarily and permanently invalidating and rescinding the BOD and the December 6, 2017, Final Decision maintaining the BOD and enjoining DHS from enforcing the BOD and the Final Decision;

(b) Declaring the BOD and Final Decision invalid, and declaring that the presence of Kaspersky Lab-branded products on federal information systems do not present a known or reasonably suspected information security threat, vulnerability, and risk to federal information systems; and

(c) Granting such other relief as the Court deems just and proper.

Dated: December 18, 2017

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