Baker & McKenzie LLP

815 Connecticut Avenue, N.W.
Washington, DC 20006-4078
United States

Tel: +1 202 452 7000
Fax: +1 202 452 7074
www.bakermckenzie.com

November 10, 2017

Ref: BOD-17-01

Department of Homeland Security
Washington, D.C. 20528

Via email
BOD.Feedback@hq.dhs.gov

CONFIDENTIAL BUSINESS INFORMATION
FOIA TREATMENT REQUESTED

Attention: Elaine C. Duke, Acting Secretary of Homeland Security

Kaspersky Lab Request for Department of Homeland Security to Initiate Review of Binding Operational Directive - 17-01

In accordance with the requirements set out in *Federal Register* / Vol. 82, No. 180 / Tuesday, September 19, 2017, and in accordance with our prior correspondence with the Office of General Counsel, please find below Kaspersky Lab's ("Kaspersky Lab" or the "Company") response ("Letter") to the U.S. Department of Homeland Security ("DHS") Binding Operational Directive 17-01 of September 13, 2017 ("BOD"),[1] the Decision Memorandum of the same date ("Decision Memorandum"),[2] and the memorandum for the Acting Secretary of DHS supporting the BOD of September 1, 2017 (the "DHS Memorandum").[3]

I. OVERVIEW

Kaspersky Lab is a market-leading defensive cyber technology company consistently recognized by its peers, the industry, and consumer groups for developing best-in-class cyber-protection tools. The Company leads the world in cyberthreat assessment and analysis. Kaspersky Lab is a key part of a global cybersecurity community, collaborating on an apolitical basis to protect all technology users from cyberthreats regardless of their origin or purpose. Kaspersky Lab takes this role and its responsibility very seriously; the Company's integrity and independence together with its stand-out technology are the foundations of its success over the past 20 years of business.

Through the BOD, DHS has sought to summarily extinguish these key contributions as well as Kaspersky Lab's hard-earned reputation, without providing constitutionally mandated due process of law.

[1] DHS BOD 17-01 (Sept. 13, 2017) [hereinafter BOD].
[2] DHS Decision Memorandum (Sept. 13, 2017) [hereinafter Decision Memorandum].
[3] DHS Information Memorandum (Sept. 1, 2017) [hereinafter DHS Memorandum].

In so doing, DHS fails to provide any evidence of wrongdoing on the part of Kaspersky Lab or anyone associated with it, much less any evidence that Kaspersky Lab presents a materially different risk profile than any other similarly situated anti-virus product or system critical software. Yet, based apparently on the nationality of the Company alone, the BOD singles out Kaspersky Lab. Such action is a clear violation of Kaspersky Lab's Equal Protection rights.

The BOD is based on a series of uncorroborated news articles and anonymous sources, none of which have been tested in a fair and public forum. Nor has Kaspersky Lab been granted an opportunity to be heard on these allegations prior to the BOD being put into effect.

Nevertheless, Kaspersky Lab has attempted in this Letter to respond to the arguments and allegations made against the Company by DHS as best it can,[4] including through the engagement of the Berkeley Research Group, LLC ("BRG") to independently review Kaspersky Lab and competitors' products and capabilities. In summary, we will show that: i) Kaspersky Lab software operates in a manner that closely aligns with the offerings of other providers not subject to the DHS action; and ii) Kaspersky Lab and its staff have no inappropriate connections to the Russian Government or its security services and pose no greater risk to the U.S. than any other company, including U.S. companies, that maintains a presence in Russia.

In particular, we wish to highlight that DHS's professed administrative procedure is wholly inadequate to meet even the minimum standards of due process. As early as July 18, 2017, Kaspersky Lab attempted to formally engage in meaningful dialogue with DHS to address its perceived concerns. Despite the clear opportunity to do so, DHS declined to engage with the Company. As a result, from the moment the BOD was issued, Kaspersky Lab began to suffer the significant adverse consequences of DHS's action in its commercial, consumer, and State, local, and education ("SLED") businesses. Furthermore, federal agencies were required to immediately begin identifying subject products on their systems and develop a plan to purge them. Constitutional due process protections of the Fifth Amendment have been consistently interpreted to require the opportunity to be heard at a meaningful time and in a meaningful manner before any action is taken to deprive a company of its protected property or liberty interests. Kaspersky Lab's rights in this regard have therefore been irreparably infringed.

The scope and breadth of the BOD is astonishing, in both effectively debarring Kaspersky Lab from all federal government contracts, and purging it from any existing engagement. But the true impact of the BOD goes far beyond the loss of limited revenue generated from Kaspersky Lab's government business and any future prospect of expanding that portfolio. Through the BOD, and other derogatory statements made by federal Government officials, DHS has taken arbitrary, capricious, and unprecedented action to single-out and seek to exclude Kaspersky Lab from the U.S. market. As a result, Kaspersky Lab has a clear cause of action to challenge the BOD under the Administrative Procedure Act ("APA").

Alongside constitutional failings, Kaspersky Lab has suffered immediate and irreparable harm to its commercial, consumer, and SLED businesses as a direct result of this action

[4] Kaspersky Lab reserves the right to produce additional material later deemed to be relevant to DHS's inquiry and concerns.

including, but not limited to, a substantial reduction in quarterly results when compared to the same time last year.

DHS has apparently given no consideration to, and certainly has not engaged with, Kaspersky Lab to discuss any reasonable measures that may address its concerns and mitigate the perceived risks inherent in the U.S. Government and others' use of Kaspersky Lab products and services.

II. BACKGROUND ON THE BOD

On September 13, 2017, DHS issued the BOD, which compels 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) begin implementing the plan within 90 days.[5] The 30-day identification deadline fell on October 13, 2017, the 60-day removal plan deadline falls on November 12, 2017, and the 90-day deadline to begin removal falls on December 12, 2017.

In issuing the BOD, DHS relied upon the Federal Information Security Modernization Act of 2014 ("FISMA"), which authorizes the Secretary of Homeland Security to develop and oversee the implementation of binding operational directives to agencies.[6] FISMA provides that a binding operational directive is a "compulsory direction to agencies" for the purpose of "safeguarding Federal information and information systems from a known or reasonably suspected[7] information security threat, vulnerability, or risk."[8]

III. BACKGROUND ON KASPERSKY LAB AND ITS U.S. GOVERNMENT BUSINESS

a. The Company and its Principles of Fighting Cyberthreats

Kaspersky Lab is a multinational cybersecurity company exclusively focused on protecting against cyberthreats, no matter their origin. From its founding, Kaspersky Lab has set out to be a leader and innovator in this space, and has been recognized as such by cybersecurity experts the world-over.[9]

Kaspersky Lab, which celebrated its 20th anniversary in 2017, is one of the world's largest privately owned cybersecurity companies, operating in 200 countries and territories and maintaining 35 offices in 31 countries, collectively with over 3,800 employees. Among its offices are research and development centers employing anti-malware experts in the U.S., Europe, Japan, Israel, China, Russia, and Latin America. More than 85 percent of Kaspersky Lab's sales are from outside of Russia. Over 400 million users, from commercial enterprise to

---

[5] BOD, *supra* note 1, at 2-3.
[6] 44 U.S.C. § 3553(b).
[7] FISMA provides no definition of the "reasonably suspected" standard, and we are unaware of any judicial or other interpretation of the standard, in this context.
[8] *Id.* § 3552(b)(1)(A). *See also* 44 U.S.C. § 3554(a)(1)(B)(ii) ("The head of each agency shall… be responsible for… complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines, including…operational directives developed by the Secretary under section 3553(b).")
[9] *See* discussion *infra* at Section III(b).

critical infrastructure owners and operators and consumers alike, utilize Kaspersky Lab technologies to secure their data and systems.

Kaspersky Lab's Global Research & Analysis Team ("GReAT"), comprised of elite security researchers located in every major region across the world, including the U.S., have been actively involved in the discovery and disclosure of numerous malware attacks. Over the past 10 years, Kaspersky Lab has identified numerous cyberthreats originating in Russia and/or operating in the Russian language,[10] many of which were specifically targeting U.S. (governmental and private) entities, including: Moonlight Maze,[11] RedOctober,[12] CloudAtlas,[13] Miniduke,[14] CosmicDuke,[15] Epic Turla,[16] Penquin Turla,[17] Turla,[18] Black Energy,[19] Agent.BTZ,[20] Teamspy,[21] Sofacy (aka Fancy Bear, APT28),[22] and CozyDuke (aka Cozy Bear, APT29).[23]

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. Kaspersky Lab believes that global collaboration is the most effective way of fighting cybercrime and protecting the privacy interests of consumers. Kaspersky Lab openly shares its expertise, knowledge and technical findings with governments, cyber-enforcers, and the information security community.

Eugene Kaspersky has consistently asserted the Company's position that governments and private sector cybersecurity companies need to cooperate to protect citizens, companies, and critical infrastructure against any and all cyberthreats regardless of their geographic origin.

---

[10] The use of Russian language (or any other) does not permit attribution of the threat to any specific country. Language traces cannot be considered reliable evidence because they can be fabricated and deliberately planted in malware code as "red herrings" for investigators.
[11] Costin Raiu, Daniel Moore, Juan Andrés Guerrero-Saade, and Thomas Rid, *Penquin's Moonlit Maze*, SECURELIST (Apr. 3, 2017), https://securelist.com/penquins-moonlit-maze/77883/.
[12] GReAT, *Cloud Atlas: RedOctober APT is back in style*, SECURELIST (Dec. 10, 2014), https://securelist.com/cloud-atlas-redoctober-apt-is-back-in-style/68083/.
[13] *Id.*
[14] GReAT, *Miniduke is back: Nemesis Gemina and the Botgen Studio*, SECURELIST (July 3, 2014), https://securelist.com/miniduke-is-back-nemesis-gemina-and-the-botgen-studio/64107/.
[15] COSMICDUKE, https://apt.securelist.com/#secondPage/attack=01.
[16] GReAT, *The Epic Turla Operation*, SECURELIST (Aug. 7, 2014), https://securelist.com/the-epic-turla-operation/65545/.
[17] Kurt Baumgartner and Costin Raiu, *The 'Penquin' Turla*, SECURELIST (Dec. 8, 2014), https://securelist.com/the-penquin-turla-2/67962/.
[18] *The Epic Turla Operation*, *supra* note 16.
[19] GReAT, *BlackEnergy APT Attacks in Ukraine employ spear phishing with Word documents*, SECURELIST (Jan. 28, 2016), https://securelist.com/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/73440/. *See generally* https://securelist.com/?s=black+energy.
[20] Alexander Gostev, *Agent.btz: a Source of Inspiration?*, SECURELIST (Mar. 12, 2014), https://securelist.com/agent-btz-a-source-of-inspiration/58551/.
[21] GReAT, *The TeamSpy Crew Attacks – Abusing TeamViewer for Cyberespionage*, SECURELIST (Mar. 20, 2013), https://securelist.com/the-teamspy-crew-attacks-abusing-teamviewer-for-cyberespionage-8/35520/.
[22] GreAT, *Sofacy APT hits high profile targets with updated toolset*, SECURELIST (Dec. 4, 2015), https://securelist.com/sofacy-apt-hits-high-profile-targets-with-updated-toolset/72924/.
[23] Kurt Baumgartner and Costin Raiu, *The CozyDuke APT*, SECURELIST (Apr. 21, 2015), https://securelist.com/the-cozyduke-apt/69731/.

Kaspersky has dubbed this philosophy "security without borders,"[24] which is consistent with the broad consensus on the need to develop international standards to govern nation-state conduct in cyberspace.

To this end, Kaspersky Lab works closely with IT security vendors, including those in the U.S., routinely taking part in joint cyberthreat investigations with such companies as Adobe,[25] Novetta,[26] AlienVault Labs,[27] Dell Secureworks,[28] Crowdstrike,[29] Honeynet Project,[30] OpenDNS Security Research Team,[31] GoDaddy Network Abuse Department,[32] Seculert,[33] SurfNET,[34] Microsoft,[35] Kyrus Tech Inc.,[36] and others.

Protecting against cyber criminals is a mission that is shared between Kaspersky Lab and many law enforcement authorities. As such, Kaspersky Lab does, from time to time, have cause to interact with law enforcement.

The Company routinely collaborates with local, regional, and international law enforcement agencies, along with the global IT security community, to fight cybercrime. Key partners include, but are not limited to, INTERPOL,[37] Europol, Microsoft Digital Crimes Unit, the National High Tech Crime Unit ("NHTCU") of the Netherlands' Police Agency, CyberSecurity Malaysia, and the City of London Police, as well as Computer Emergency Response Teams ("CERT"s) worldwide. Kaspersky Lab works closely with these organizations, providing technical expertise and forensic analysis of malicious programs, during investigations and in compliance with court orders.

---

[24] *See* Eugene Kaspersky, *Security Without Borders*, FORBES, Mar. 18, 2015, https://www forbes.com/sites/eugenekaspersky/2015/03/18/security-without-borders/#68b70d8010d6, and Eugene Kaspersky, A Digital Geneva Convention? A Great Idea., FORBES, Feb. 15, 2017, https://www forbes.com/sites/eugenekaspersky/2017/02/15/a-digital-geneva-convention-a-great-idea/#24c682f51e6e.

[25] GReAT, *BlackOasis APT and new targeted attacks leveraging zero-day exploit*, SECURELIST (Oct. 16, 2017), https://securelist.com/blackoasis-apt-and-new-targeted-attacks-leveraging-zero-day-exploit/82732/.

[26] Kaspersky Lab, *Kaspersky Lab helps to disrupt the activity of the Lazarus Group responsible for multiple devastating cyber-attacks* (Feb. 25, 2016), https://www.kaspersky.com/about/press-releases/2016_kaspersky-lab-helps-to-disrupt-the-activity-of-the-lazarus-group-responsible-for-multiple-devastating-cyber-attacks.

[27] *Id.*

[28] Kaspersky Lab, *How Kaspersky Lab and CrowdStrike Dismantled the Second Hlux/Kelihos Botnet: Success Story* (Mar. 28, 2012), http://newsroom kaspersky.eu/en/texts/detail/article/how-kaspersky-lab-and-crowdstrike-dismantled-the-second-hluxkelihos-botnet-success-story/.

[29] *Id.*

[30] *Id.*

[31] Kaspersky Lab, *Kaspersky Lab Experts Provide In-Depth Analysis of Flame's C&C Infrastructure* (June 3, 2012), https://usa kaspersky.com/about/press-releases/2012_kaspersky-lab-experts-provide-in-depth-analysis-of-flame-s-c-c-infrastructure.

[32] *Id.*

[33] Kaspersky Lab, *Kaspersky Lab and Seculert Announce 'Madi,' a Newly Discovered Cyber-Espionage Campaign in the Middle East* (July 17, 2012), https://me-en.kaspersky.com/about/press-releases/2012_kaspersky-lab-and-seculert-announce--madi--a-newly-discovered-cyber-espionage-campaign-in-the-middle-east.

[34] Kaspersky Lab, *Kaspersky Lab, Kyrus Tech and Microsoft Disable the Hlux/Kelihos Botnet* (Sept. 30, 2011), http://newsroom.kaspersky.eu/en/texts/detail/article/kaspersky-lab-kyrus-tech-and-microsoft-disable-the-hluxkelihos-botnet/?no_cache=1&cHash=f0887050ffe60599c57cf0073b860dec.

[35] *Id.*

[36] *Id.*

[37] *See*, for example, *infra* note 174.

Kaspersky Lab has worked with the National Security Agency ("NSA"), DHS U.S. Computer Emergency Readiness Team ("US-CERT") and Industrial Control Systems Cyber Emergency Response Team ("ICS-CERT"), Department of State, and other key elements of the U.S. Government involved in protecting U.S. cyberspace.

In particular Kaspersky Lab and its staff and management have:

- briefed DHS officials on findings related to cyberthreats, often before they were made public, in addition to sharing vulnerability research with US-CERT and ICS-CERT;
- communicated with NSA regarding threats found;
- briefed relevant Congressional and Senate Committees of jurisdiction (including the Committee on Homeland Security, the Committee on Homeland Security and Governmental Affairs, the Permanent Select Committee on Intelligence, the Select Committee on Intelligence, the State Department's Bureau of Diplomatic Security, and others); and
- participated in Congressional staff briefings on ransomware.

In 2016, Kaspersky Lab assisted in Russia's largest cybercriminal investigation and ultimate arrest of hackers known as the "Lurk Gang" who stole $45 million from banks, other financial institutions, and businesses.[38] Kaspersky was also instrumental in identifying and pursuing the "Carbanak cybercrime gang," which targeted dozens of global financial institutions, stealing a total of $1 billion.[39]

b. Global Recognition by its Peers

Kaspersky Lab has been consistently recognized in the industry and by its peers as a premier organization in the fight against malware and cyber crime. Kaspersky Lab products consistently rank in the top tier of anti-virus products.[40] In 2016, Kaspersky Lab products participated in 78 independent tests & reviews – and was awarded 55 first places and 70 top-three finishes.[41] Kaspersky Lab consistently ranks among the world's top four vendors of security solutions for endpoint users.[42]

The origin of its sales and revenue, both closely tied to its neutrality, alongside these examples of Kaspersky Lab's commitment to protecting its users from cyberthreats and

---

[38] *See* Kaspersky Lab, *Kaspersky Lab Assists in Russia's Largest Cybercriminal Arrest: The Hackers Who Stole $45 Million* (June 1, 2016), https://usa.kaspersky.com/about/press-releases/2016_kaspersky-lab-assists-in-russia-s-largest-cybercriminal-arrest-the-hackers-who-stole--45-million.

[39] *See* New York Times, *Bank Hackers Steal Millions via Malware* (February 14, 2015) https://www nytimes.com/2015/02/15/world/bank-hackers-steal-millions-via-malware html and Kaspersky Lab, *The greatest heist of the century: hackers stole $1 bln* (February 16, 2015), https://www kaspersky.com/blog/billion-dollar-apt-carbanak/7519/.

[40] *See* BRG Assessment, *infra* note 55, at 32.

[41] Kaspersky Lab, *Most Tested. Most Awarded. Kaspersky Lab Protection*, https://usa kaspersky.com/top3 (last visited Nov. 6, 2017).

[42] Frank Dickson, Robert Westervelt, and Maureen Kelledy, *Worldwide Endpoint Security Market Shares, 2016: Competition Gets Fierce, # US42553717*, INTERNATIONAL DATA CORPORATION, May 2017, https://www.idc.com/getdoc.jsp?containerId=US42553717.

preventing cybercrime, run contrary to any suggestion that the Company would engage in the activities alleged and speculated upon in the press articles forming the basis of DHS's conclusions reflected in the BOD.

c. Corporate Structure

Like many international companies, Kaspersky Lab has a multi-national operating company structure with regional holding companies ultimately deriving up to Kaspersky Labs Limited ("KLL"), a U.K. company. The co-founder and current Chief Executive Officer of Kaspersky Lab, Eugene Kaspersky, personally holds over 80 percent of KLL's stock in the U.K. The remainder of KLL stock is held by individuals, principally those who trace their stock ownership back to the early days of the Company when they were granted a share in its ownership. Currently, there are no outside corporate investors.

Kaspersky Lab has its global headquarters in Moscow, operating through the Russian corporation, AO Kaspersky Lab. AO Kaspersky Lab is 100 percent owned by KLL through the Russian corporation, OOO Kaspersky Group. In addition to its global headquarters, Kaspersky Lab has five regional headquarters managing the company's sales and operations across six continents, including in its North American HQ (Woburn, MA), Latin American HQ (São Paolo, Brazil), European HQ (London, U.K.), Middle East, Turkey & Africa HQ (Dubai, UAE), and Asia-Pacific HQ (Singapore).

Founded in 2004, Kaspersky Lab, Inc. is a Massachusetts corporation and is a directly wholly-owned subsidiary of KLL. There are no Russian companies in the ownership structure of Kaspersky Lab, Inc., which employs nearly 300 people in the U.S. The Company's North American sales and operations are driven through Kaspersky Lab, Inc., which has invested over half a billion dollars in the Company's operations over the last twelve years, and over $65 million in 2016 alone. The U.S. has been and remains one of the most significant geographic markets in Kaspersky Lab's global business, with Kaspersky Lab sales to customers in the United States representing approximately one quarter of total global bookings in 2016.

d. Kaspersky Lab's Sales to U.S. Government

All Kaspersky Lab U.S. operations and sales are driven through Kaspersky Lab, Inc., with its North American headquarters in Woburn, Massachusetts. Consistent with the practice of most software companies, Kaspersky Lab operates a two-tier channel sales model by which it sells Kaspersky Lab products to customers through distributors and resellers. Kaspersky Lab has no visibility into the terms of any sales that its resellers may make to federal agencies.[43]

Through an analysis of sales data, Kaspersky Lab has identified active licenses held by federal agencies with a total value (to Kaspersky Lab) of less than USD $54,000. More than half of these U.S. Government customer sales (in terms of dollar value) were booked before 2017 and are continuing multi-year licenses. The total value of these licenses held by the U.S.

[43] For sales tracking purposes (i.e. to calculate revenue due from its distributors), Kaspersky Lab tracks customer sales volumes and active licenses through its Salesforce Customer Relationship Management system. Although Kaspersky does identify customers by industry (including identifying government customers), it does not specifically identify Federal Government Customers distinct, for example, from state and local government entities.

Government represents a tiny fraction (0.03 percent) of Kaspersky Lab's annual revenue in the U.S.[44]

In summary, Kaspersky Lab has never specifically sought out federal government agencies as software customers, has always relied on the sales channel to identify and pursue sales leads in both the private and public sector, and works to enable its partners to realize each and every sales opportunity regardless of its target.

As a result, Kaspersky Lab has a very limited customer base within the U.S. Government. It is common that a potential customer, whether governmental or private, will receive several quotes for similar product offerings from a variety of security vendors, and the customer will make its decision to procure one product over another for a variety of reasons, including price terms, reputation, system compatibility, and integration with other solutions the customer may have. From information provided by the partners making the relevant sales, we understand that some U.S. Government customers have actively sought out Kaspersky Lab products because of their renowned anti-malware capabilities,[45] while others have specifically approached resellers for solutions due to Kaspersky Lab's legacy platform support. For instance, Kaspersky Lab protects older operating systems, such as Windows XP, for which other cybersecurity vendors have ceased providing support.

Kaspersky Lab incorporated and launched Kaspersky Government Security Solutions Inc. ("KGSS"), a subsidiary of Kaspersky Lab, Inc., in May 2014. From its inception, KGSS focused on delivering cyberthreat intelligence and data feeds[46] (similar to the Kaspersky Threat Intelligence product expressly excluded from the scope of the BOD). Following its establishment, KGSS undertook a number of marketing initiatives including holding an annual Government Cybersecurity Forum in Washington, D.C. in 2014 and 2015. Despite these efforts, KGSS never made any sales of Kaspersky Lab products or services to the U.S. Government.

By early summer 2017, KGSS' sales and marketing efforts to the U.S. Government were discontinued. Prior to then, business plans had been developed (with no relation to KGSS's business model and product offerings at the time) to monetize Kaspersky Lab's cyberthreat intelligence blog (threatpost.com), and a decision was made to incorporate an additional legal entity in the U.S. in order to manage the business development and operations of the Threatpost blog. In the interest of operational efficiency, rather than incorporating a new U.S. company to take on the Threatpost project, it was decided that the corporation, then known as KGSS, simply be renamed to Threatpost, Inc. such that the already incorporated U.S. legal entity be repurposed in line with the new business plans. In July 2017, KGSS was renamed Threatpost, Inc., which manifests a completely new business model, unrelated to any of KGSS' previous activities.

IV. OVERVIEW OF KASPERSKY LAB PRODUCTS SUBJECT TO THE BOD

Kaspersky Lab tracks more than 100 advanced persistent threat actors and operations and has a broad portfolio of products that encompass solutions to suit a wide range of customers.

---

[44] This figure is based on the Company's 2016 net booking data.
[45] *See* discussion *infra* at Section.III.b)
[46] *See* Exhibit A, KGSS Cyber Threat Intelligence Product Catalogue from August 2016.

Kaspersky Lab protects home users, enterprises of all sizes, government customers, and others from hugely dynamic cyberthreats through its cost competitive products that allow customers to control and manage their security. For complex corporate, enterprise, and government customers, Kaspersky Lab offers an assortment of solutions and services that secure every node in the network, including mobile and portable devices, data centers, and industrial environments as a whole.

Kaspersky Lab is now, and has always been, ready, willing, and able to provide DHS with any and all further technical data to allow DHS to independently assess the functionality of these products and their integrity. For the reasons explained below, DHS should provide (and should have already provided) Kaspersky Lab with the opportunity to address DHS's concerns and whether they might be mitigated prior to harming Kaspersky Lab's existing property, liberty, and reputational interests.

DHS lists the following Kaspersky Lab products subject to the BOD:[47]

- Kaspersky Anti-Virus;
- Kaspersky Internet Security;
- Kaspersky Total Security;
- Kaspersky Small Office Security;
- Kaspersky Anti Targeted Attack;
- Kaspersky Endpoint Security;
- Kaspersky Cloud Security (Enterprise);
- Kaspersky Cybersecurity Services;
- Kaspersky Private Security Network; and
- Kaspersky Embedded Systems Security.

Kaspersky Lab has not been made aware of how or under what criteria DHS evaluated and compiled this product list, though it appears to have been from a cursory review of the Company's website rather than any substantive review or technical assessment of the individual products. [48] What is clear is that neither this list (nor the inconsistent list contained in the DHS Memorandum),[49] is an accurate rendering of Kaspersky Lab products. For example, neither "Kaspersky Cloud Security (Enterprise)" nor "Kaspersky Cybersecurity Services" represent discrete product offerings the Company makes available. This demonstrates a lack of awareness and understanding of the Kaspersky Lab product portfolio and therefore, we assume also the functionality of many of those products.

Kaspersky Lab does welcome the acknowledgement that Kaspersky Threat Intelligence[50] and Kaspersky Security Training[51] are services of a different category to its anti-virus offerings and therefore have been excluded from the scope of the BOD. However, by including "Kaspersky Cybersecurity Services" on the list of products and services subject to the BOD, which is not a discrete product in its own right, DHS has simultaneously prohibited the

[47] BOD, *supra* note 1, at 2.
[48] DHS Memorandum, *supra* note 3, at 5 ("Based on a review of Kaspersky's website, all of the following software products or solutions named in the BOD are or contain anti-virus software.")
[49] DHS Memorandum, *supra* note 3, at 5.
[50] Kaspersky Threat Intelligence is a subscription-based periodic cyberthreat intelligence publication.
[51] Kaspersky Security Training is a cyber security training program.

procurement of these services since both (and others) could be considered to fall under the umbrella description of "Cybersecurity Services."

The BOD also applies to any other information security product or solution not explicitly named in the BOD, which is supplied, directly or indirectly, by any Kaspersky Lab entity as well as to all cybersecurity services supplied, directly or indirectly, by Kaspersky Lab, including Threat Hunting, Incident Response, and Security Assessment. As noted above, DHS alleges that "Cybersecurity Services" also supplied by Kaspersky Lab presents various information security risks, even if the services do not involve installation of anti-virus software.

DHS's allegations are conclusory and rely solely on a general statement in the Information Security Risk Assessment, prepared by DHS National Cybersecurity and Communications Integrations Center ("NCCIC"), dated August 29, 2017, (the "NCCIC Assessment")[52] that "any service that involves direct or indirect access to a computer or network, such as through installation of endpoint software to conduct a 'hunt' or incident response, or through other abilities to influence information security practices on a network, presents information security risks."[53] A conclusory allegation that Kaspersky Lab services present the same information security risks as "any service that involves direct or indirect access to a computer or network" is anything but a sufficient basis for a comprehensive ban on all Kaspersky Lab branded products and services.[54]

In order to address the concerns raised in the BOD regarding the capabilities and alleged vulnerabilities of Kaspersky Lab's products, Baker McKenzie retained cybersecurity professionals at BRG to:

- review the methodology employed by DHS in its issuance of the BOD, which concluded that Kaspersky-branded products, in particular, represent an information security risk to federal information systems; and

- provide an independent expert review and assessment of any technical information security risks described in the BOD or its supporting materials related to Kaspersky-branded products or other anti-virus software products in general.

Attached hereto as Exhibit B are the results of BRG's independent review, titled "Information Security Risks of Anti-Virus Software" (the "BRG Assessment")[55] and the findings of BRG's Assessment are further described at Section V. below.

V. BRG INDEPENDENT TECHNICAL ASSESSMENT OF KASPERSKY LAB AND COMPETITOR PRODUCTS

The risks that Kaspersky Lab products present to the U.S. Government as alleged in the NCCIC Assessment are broadly categorized as follows:[56]

---

[52] DHS Memorandum, *supra* note 3, at Exhibit 1.
[53] DHS Memorandum, *supra* note 3, at 7.
[54] *Id.*
[55] *See* Exhibit B, Berkeley Research Group, *Information Security Risks of Anti-Virus Software: Independent Review of DHS 17-01* (Nov. 10, 2017) [hereinafter BRG Assessment].

- anti-virus software products generally operate with the highest level of system privileges and could theoretically be co-opted by the anti-virus software vendor or other malicious parties (e.g. via exploitation of a software vulnerability) into performing unintended actions of the user's computer (e.g. data exfiltration);

- anti-virus software products often intercept encrypted HTTPS traffic on the user's computer for the purposes of identifying or preventing malicious network traffic, which defeats the intended purpose of HTTPS;

- any software that receives unencrypted updates over the network could be hijacked or otherwise tampered with in order to deliver malicious code to the user's computer; and

- anti-virus software vendors, in particular, could withhold legitimate software or anti-virus signature updates in order to intentionally prevent detection of malicious software.

Each area of concern is considered below.

a. DHS Fails to Identify any Technical Information Security Vulnerability Specific to Kaspersky-Branded Products

The BRG Assessment notes that DHS presented no evidence to demonstrate (i) that NCCIC performed a technical analysis of Kaspersky Lab products, or (ii) that Kaspersky Lab products (or any other commercial off-the-shelf ("COTS") anti-virus product) have been subjected to (or leveraged for) any of the above-stated risks.[57]

Among other things, BRG analyzed data from USASpending.gov, a website that aggregates federal government contract data and found references to federal government anti-virus software product purchases from approximately 30 different developers over the past 10 years.[58] Based on this data, BRG selected anti-virus products from six other vendors to review: Symantec, McAfee, Trend Micro, Avast, AVG, and ESET.[59]

BRG conducted a search of publicly reported vulnerabilities to determine whether these products may be (or have been) exploitable by malicious actors.[60] In the past five years, security researchers have identified numerous vulnerabilities in software developed by each of the vendors listed above. In addition, BRG's review identified several instances in which hackers have been able to compromise some of the anti-virus companies themselves.

Although most of the publicly-disclosed vulnerabilities were reported by security researchers, it is reasonable to infer that sophisticated state-sponsored actors with substantial resources

---

[56] DHS Memorandum, *supra* note 3, at 5-6.
[57] *See* BRG Assessment, *supra* note 55, at 6.
[58] *See* BRG Assessment, *supra* note 55, at 9-10. Despite the information security concerns identified by DHS in the BOD, BRG concluded that the U.S. Government does not have a consistent approach to the identification, evaluation, procurement, and deployment of anti-virus software across its various departments and agencies.
[59] *See* BRG Assessment, *supra* note 55, at 10.
[60] *See* BRG Assessment, *supra* note 55, at 11.

would have the same ability to identify and exploit similar vulnerabilities in any anti-virus software product.

BRG concluded that neither the NCCIC Assessment nor the DHS Memorandum 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."[61] Rather BRG, through its own work, concluded that other anti-virus software products are just as vulnerable to exploitation by malicious cyber actors as DHS alleges is the case for Kaspersky-branded software products.[62]

DHS has not, however, issued a similar ban on the use of any of these other products within government networks or information systems.

b. Potential Software Vulnerabilities Are Not Limited To Anti-Virus Products

In addition to anti-virus products, there are other applications commonly found on federal information systems that are vulnerable to security risks, which could equally result in the execution of arbitrary code or commands on a victim's computer.[63] Examples of these applications include: web browsers, Microsoft Office products, and the Microsoft Windows operating system. In addition, even "enterprise-level hardware products responsible for enforcing the security of a network have been found to contain vulnerabilities that can be leveraged by a malicious actor to gain unauthorized access to data or systems."[64]

If one were to accept DHS's conclusion that a particular software product or vendor should be banned because of its presumed susceptibility to exploitation by a malicious actor, that same conclusion should reasonably be extended to other software products beyond anti-virus software or other vendors besides Kaspersky Lab.[65]

c. Kaspersky Lab's Data Collection Practices are Similar to Other Manufacturers of Off the Shelf Anti-Virus Products Used by the U.S. Government

The only alleged information security risk identified in the DHS Memorandum and the NCCIC Assessment that could be unique to Kaspersky Lab (as opposed to broadly describing COTS anti-virus functionality) relates to customer participation in the Kaspersky Security Network ("KSN")."[66]

However, instead of conducting a technical analysis of the operation of KSN, DHS focuses on the terms and conditions set forth in the KSN "Statement for Kaspersky Endpoint Security 10 for Windows" (the "KSN Statement").[67]

---

[61] *See* BRG Assessment, *supra* note 55, at 6.
[62] *See* BRG Assessment, *supra* note 55, at 12.
[63] *See* BRG Assessment, *supra* note 55, at 7.
[64] *See* BRG Assessment, *supra* note 55, at 7.
[65] *See* BRG Assessment, *supra* note 55, at 7.
[66] DHS Memorandum, *supra* note 3, at 6.
[67] DHS Memorandum, *supra* note 3, at 7, fn. 18.

In particular, if an end-user chooses to participate in KSN, the KSN Statement includes terms that could permit Kaspersky Lab to collect files or other information from a user's device and upload it to the KSN. However, the KSN is not alone in transferring the type of data enumerated above; many other anti-virus software vendors maintain their own networks for providing malware signature updates to users and collecting samples of suspected malware.

BRG reviewed the End User License Agreement ("EULAs") and/or Privacy Policy documents for the six additional anti-virus products listed above that are used by the U.S. Government: Symantec, McAfee, Trend Micro, Avast, AVG, and ESET.[68]

BRG found that nearly every anti-virus product or vendor includes similar or, in some cases (e.g. McAfee), broader allowances for data collection compared to the KSN Statement cited in the DHS Memorandum as an information security risk.[69] Based on this review, BRG concluded that this particular information security risk is not, in fact, unique to Kaspersky Lab and its KSN Statement. Indeed, the number of other anti-virus software providers transferring similar data from its users demonstrates the ubiquity of this practice and shows how Kaspersky Lab, alongside other anti-virus software providers, is following industry practice in user data collection.

For example, similar to how KSN users agree to provide whole files or parts of files that could be exploited by intruders to harm a user's computer, McAfee,[70] Avast CommunityIQ,[71] ESET,[72] TrendMicro,[73] AVG,[74] and Norton Security[75] users also agree to provide files that

---

[68] *See* BRG Assessment, *supra* note 55, at 16-20.
[69] *See* BRG Assessment, *supra* note 55, at 16.
[70] "McAfee Privacy Notice." Privacy & Legal Terms, McAfee, LLC, 4 Apr. 2017, www mcafee.com/consumer/en-us/policy/global/legal html. ("The following are examples of the type of Usage Data that may be collected by McAfee from your web browser or related to your interactions with our products and services:… Data about files and communications, such as potential malware or spam (which may include computer files…).
[71] "Avast Privacy and Information Security Policy." Avast Privacy Policy, AVAST Software S r.o., www.avast.com/en-us/privacy-policy ("Data acquired by Avast CommunityIQ is used to update our databases of viruses and infected websites, and for other statistical purposes, and may include: Information and files (including executable files) on your computer identified by the Avast software as potentially infected, together with the information about the nature of identified threats.")
[72] "Software End User License Agreement." ESET, ESET Spol. s R.o., www.eset.com/us/software-eula/. ("The Software contains a function which collects samples of new viruses and other similar malicious programs and suspicious or problematic files (hereinafter referred to as "Infiltrations") and then sends them to the Provider, along with information about the computer and/or the platform on which the Software is installed (hereinafter referred to as "Information")…The Information may contain data (including randomly or accidentally obtained personal data) about the End User and/or other users of the computer on which the Software is installed, information about the computer, the operating system and programs installed, files from the computer on which the Software is installed and files affected by an Infiltration and details about such files.")
[73] "Privacy Notice for Trend Micro Products and Services (Effective Jan. 2017)." Trend Micro, Trend Micro Incorporated, Jan. 2017, www.trendmicro.com/en_us/about/legal/privacy-policy-product html. (Providing these types of information and data enables you to participate, share and leverage Trend Micro's global database of threat related intelligence to rapidly identify and defend against potential threats within your unique network environment, as described in more detail below:… detected malicious file information and detected malicious network connection information.")
[74] "Privacy Policy | We Are Serious about Your Privacy | AVG." AVG.com, AVG Technologies, 23 Mar. 2017, www.avg.com/en-us/privacy. ("We collect non-personal data to improve our products and services, including: data concerning potential malware threats to your device and the target of those threats, including copies of files or emails marked as potential malware…")

are identified as potential malware and could be exploited by intruders to harm the user's computer.

d. Use of the KSN Network is Optional

KSN is an automated cloud-enabled system that processes depersonalized cybersecurity-related data streamed from millions of voluntary participants around the world. Kaspersky Lab uses this data to identify emerging threats more quickly and precisely to develop and implement new protection measures as quickly as possible. For example, the data that Kaspersky Lab processes is crucial for identifying new and as yet unknown threats – such as WannaCry and ExPetr. All data transferred via the KSN is aggregated and anonymous; Kaspersky Lab does not attribute data to identified individuals. In addition, all data processed and/or transferred is robustly secured through encryption, digital certificates, segregated storage, and strict data access policies.

As noted by DHS, a customer's participation in the KSN program is entirely voluntary. If a customer does not wish to participate, the terms of the KSN Statement would not apply but nonetheless a small amount of data is shared as it is essential for the product to function properly. This data is used to verify the legitimacy of the products, send database updates, and keep them operational.

As detailed on the Kaspersky Lab website, "users of Kaspersky Lab products can reduce the amount of data processed from their protected devices to the absolute minimum."[76] In addition, the EULA for Kaspersky Anti-virus provides as follows:

> In order to identify new information security threats and their sources, enhance the operational protection of Users of the Software, and improve the quality of the product, You agree to automatically provide Kaspersky Lab with information specified in the Terms of Use of Kaspersky Security Network…You can activate and deactivate the Kaspersky Security Network service at any time in the Software settings window.[77]

Accordingly, the EULA for Kaspersky Anti-virus does not allow for the collection of files without the KSN enabled. In its Assessment, BRG noted that EULA terms are consistent with internal software documentation provided to BRG by Kaspersky Lab for review.[78]

---

[75] "Norton License Agreement." Norton Security / Norton Security with Backup, Symantec Corporation, www.symantec.com/content/en/us/home_homeoffice/media/eula/NS_2.0_EULA_USE.pdf ("From time to time, the Software and Services may collect certain information, including personally identifiable information, from the Device on which it is installed, which may include: Executable files and files that contain executable content that are identified as potential malware, including information on the actions taken by such files at the time of installation. These files are submitted to Symantec using the Software and Service's automatic submission function.")

[76] Kaspersky Lab, *Principles for the processing of user data by Kaspersky Lab security solutions and technologies,* https://www kaspersky.com/about/data-protection (last visited Nov. 6, 2017).

[77] Kaspersky Lab, *Kaspersky Anti-Virus 2013: End User License Agreement for Kaspersky Anti-Virus* (Mar. 19, 2013), https://support kaspersky.com/8752.

[78] *See* BRG Assessment, *supra* note 55, at 17.

As such, government users (as all users) have the option to disable KSN and would be an option to mitigate some of the concerns raised by the DHS. This does not appear to have been fully considered in the BOD or the DHS Memorandum.

e. Kaspersky Private Security Network

Business and government users may choose to install a local and Kaspersky Private Security Network, which allows them to obtain the advantages of cloud protection without any data leaving the user's facility.

However, the NCCIC Assessment states that this too presents a security risk by alleging that it "still does not address threats posed by the software itself as an on-premise solution" because users are required to update the on-premise software with updates provided by the software manufacturer.[79] However, DHS's allegations are purely theoretical, speculative, and conclusory.

Further, the concerns raised by DHS are present with any anti-virus solution and fail to give proper consideration to how any reasonable security risks with any anti-virus product could be mitigated. Should an anti-virus software developer intentionally withhold certain malware signatures from the U.S. Government in order to prevent detection of specific malicious software, then such a risk could be mitigated by following the guidelines published by the U.S. National Institute of Standards and Technology ("NIST") in 2013, wherein NIST recommended that this particular vulnerability could be mitigated by multiple layers of anti-virus protection at the host and network level.[80]

VI. RUSSIA AND KASPERSKY LAB'S GLOBAL FOOTPRINT

As a private company, Kaspersky Lab does not have inappropriate ties to any government, and the Company has never helped, and has repeatedly stated it *will never* help any government in the world with cyberespionage efforts.[81] For 20 years, Kaspersky Lab has focused on protecting consumers and organizations from cyberthreats. The location of its headquarters does not change that core mission.

a. Kaspersky Lab is Not an Arm of the Russian Government; It is a Successful Multi-National Private Enterprise

The DHS Memorandum has singled out Kaspersky Lab, not because of issues that are specific to Kaspersky Lab products and services, but simply because it is a company headquartered in Russia. In the absence of any evidence of improper coordination between Kaspersky Lab and the Russian Government in furtherance of demonstrable illicit activities, it is improper for DHS to speculate that cybersecurity risks are presented by Kaspersky Lab products merely by virtue of the fact that the Company is headquartered in Moscow.

---

[79] *See* DHS Memorandum, *supra* note 3, at Exhibit 1.
[80] *See* BRG Assessment, *supra* note 55, at 35 (citing http://nvlpubs nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf).
[81] *See* e.g. *Richard Engel Interview with Eugene Kaspersky*, MSNBC, July 28, 2017, http://www msnbc.com/rachel-maddow/watch/russian-kaspersky-labs-faces-new-scrutiny-suspicion-1012640835507 at 15:18.

As noted previously, all group companies (including Kaspersky Lab, Inc.) roll up to the U.K. holding company KLL, without Russian corporate ownership. DHS's stated concern that the Russian Government engages in cyberespionage is not evidence that any, or all, global companies headquartered, or with operations, in Russia pose the same threat or are necessarily facilitating government sponsored cyber-intrusions.

In excess of 85 percent of Kaspersky Lab's revenue comes from outside of Russia and, therefore, working inappropriately with the Russian Government would clearly be detrimental to the Company's bottom line. Kaspersky Lab has a powerful economic incentive to never take 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.

Rather, Kaspersky Lab's commercial and business rationale dictates that it should do everything in its power to resist and defend against all known cyberthreats and malicious cyber actors regardless of their location origin or allegiance. This is exactly the approach that Kaspersky Lab takes.[82]

Kaspersky Lab's U.S. Government business represents a tiny fraction of its U.S., much less its global, business and software footprint.[83] If DHS is concerned that the Russian Government (or any malicious cyber actor), intended to seek sensitive U.S. Government information, there would be far more direct, targeted, and effective mechanisms for them to do so. It would be much more effective, for example, for a malicious cyber actor to target and compromise a company with a larger footprint across U.S. Government and cyber defense infrastructure. As BRG concluded, other anti-virus software products, including Symantec and McAfee, are likely as vulnerable to exploitation by malicious cyber actors as DHS alleges is the case for Kaspersky-branded software products and have a much larger footprint across federal Government systems.[84]

b. Kaspersky Lab Management

The DHS Memorandum alleges that Kaspersky Lab Chief Executive Officer Eugene Kaspersky, Chief Legal Officer Igor Chekunov, and Chief Operating Officer Andrey Tikhonov have "ties" with the Russian Government and highlights, among other things, their former service within the Russian Government and/or military and their current profiles and connections.

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 kind 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.

Similarly, today, each of these individuals has found great success through Kaspersky Lab and other commercial endeavors. Given their profile, it is hardly surprising that in Russia (as

[82] *See* discussion *infra* at Section III.a.
[83] *See* discussion *infra* at Section III (d).
[84] *See* BRG Assessment, *supra* note 55, at 11.

in the U.S.) such individuals might have acquaintances, friends, and professional relationships within the government. That in itself is not indicative that any such relationship is improper, or would cause Kaspersky Lab employees or management to betray their obligations to the Company, its fundamental philosophy, or its users, to whom each has dedicated a substantial part of their working lives.

Among other things, DHS relies on a newspaper article that states that Kaspersky Lab's then Chief Business Officer, Garry Kondakov, circulated an email saying that the "company's highest positions" would be held only by Russians.[85] Kaspersky Lab has no such policy, but given that its headquarters is in Russia, the majority of the Company's senior management do clearly happen to be located there.

i. Eugene Kaspersky

Eugene Kaspersky has been the CEO of Kaspersky Lab since 2007. Prior to 2007 Eugene held various titles at the company including, "*Director of Innovation Technologies," "Senior Antivirus Expert,"* and "*Head of Division*."

During the Soviet era, every educational opportunity was endorsed by the government in some manner. After graduating from a prestigious high school with a focus in mathematics, Eugene then studied cryptography at a university overseen by four state institutions, one of which was the KGB, the Soviet intelligence service which was dissolved and reorganized in 1991. After graduating in 1987, Eugene performed his mandatory military service at a Ministry of Defense scientific institute, where he served as a software engineer. Serving as a software engineer was the extent of his military experience, and he never worked for the KGB.

In 1991, the year the Soviet Union dissolved, Eugene left the research institute and formed a small anti-virus division at an emerging commercial company. A few years later, he and a small group of associates founded Kaspersky Lab in 1997.

ii. Igor Chekunov

Igor Chekunov joined Kaspersky Lab in 2000 as the group Chief Legal Officer. Igor graduated from the Institute of Economics and Law in Moscow and has a Ph.D. in Law from the Moscow University of the Ministry of Internal Affairs of the Russian Federation, where he also currently teaches in the law department on subjects such as criminal law and procedure, criminology and cybercrime forensics.

Prior to joining Kaspersky Lab, Igor held a number of civilian positions in the legal departments of the Russian Ministries of Industry, Oil and Energy, and Transport. Igor's last position in the government was as head of the legal department at the Ministry of Transport of the Russian Federation, which is analogous to the U.S. Department of Transportation.

As a young man, Igor was required to serve in the Border Service in the Soviet Union, fulfilling his obligatory military service for two years between 1984 and 1986. At that time, the Border Service was under the remit of the KGB. In the U.S. this would be equivalent to

[85] *See* DHS Memorandum, *supra* note 3, at Exhibit 26.

working for Customs and Border Protection under DHS. After completing his compulsory service with the Border Service, Igor worked as a police officer.

Again this conscripted service, more than 30 years ago, has no relation to or bearing on Mr. Chekunov's current role as the Chief Legal Officer of a multinational commercial enterprise, Kaspersky Lab.

iii. Andrey Tikhonov

Andrey Tikhonov was appointed Kaspersky Lab's Chief Operating Officer in January 2012. In his position, Andrey is responsible for the Company's global administrative functions.

Andrey graduated with distinction from a military academy in Kiev. He has been working in the IT industry since 1989, when he began his career in a research institute of Russian Ministry of Defence.

Prior to his current role, Andrey held a number of senior management positions at Kaspersky Lab. In March 2009, he was appointed Chief Information Officer after five years as the Company's Technical Director. Before that, Andrey was head of the Novell development department since 2002.

c. Kaspersky Lab has a Limited Number of Government Customers in Russia, the U.S., and Around the Globe

As highlighted above,[86] Kaspersky Lab products and services lead the market in cyber security, anti-virus, and threat analysis. In addition to its many millions of private customers, government customers wishing to secure their own data and infrastructure turn to Kaspersky Lab products and services in the same way, and for the same reasons commercial and private customers do: Kaspersky Lab products' superior technical capabilities.

The DHS Memorandum cites news articles[87] discussing an alleged 2009 project in which Kaspersky Lab is said to have developed a defensive product to protect against disruptive denial of service security (DDoS) technology with or for the Russian Security Services. It is unclear how this allegation is relevant to the BOD and DHS's determination since anti-DDoS technology is defensive security software, not malware. Such an engagement if it were to be true, would be anything but inappropriate given Kaspersky Lab's technology and expertise. To be clear however, the Federal Security Service, also known by its Russian acronym FSB, is not currently, and never has been, a Kaspersky Lab DDoS Protection client. In the mid-to-late 2000's, Kaspersky Lab was already working on a commercial anti-DDoS offering and was engaging customers, prospects, and channel partners on this type of solution. In that context, the Russian Government's anti-cybercrime unit told the company that it considered DDoS attacks an emerging and serious threat. Since there was a strong market need, Kaspersky Lab invested in the research and development necessary to finish fully developing the solution and make it available commercially.

[86] *See* discussion *infra* at Section III.b.
[87] *See* DHS Memorandum, *supra* note 3, at Exhibit 20.

d. FSB Authority to Compel or Request Assistance from Companies in Russia

All companies represented in Russia have a general obligation to provide the FSB with such information as may be required by the FSB to perform its duties.[88] The FSB has defined duties enumerated by law, including:

- informing state authorities of security threats;
- detecting and preventing foreign intelligence activities;
- obtaining intelligence information in the interests of state security, increasing the state's economic, scientific, technical and defense capability;
- revealing and preventing violations and crimes;
- developing anti-bribery measures;
- providing for various types of security of the Russian Federation;
- developing and implementing measures to protect state secrets; and
- taking measures to protect the Russian state border.[89]

The FSB can request information from companies represented in Russia only in furtherance of the above-listed duties. If a company operating in Russia receives a request from the FSB for information, it must comply with such request. However, the FSB's powers in this regard are not unlimited, and FSB requests are subject to challenge in court.[90]

The authority of the FSB to compel or request assistance from companies in Russia, including any foreign company operating in Russia, applies regardless of the company's ownership structure, legal form, or business (as opposed, for example, to the specific obligations of Russian telecommunications providers and internet communications companies discussed below).

Similar laws exist in the U.S. to compel companies to hand over customer data and any other information. In fact, the U.S. Department of Justice has recently expressed a desire to expand its own powers in this regard to mandate technology companies to hand over encryption keys to law enforcement.[91]

---

[88] Federal Law of the Russian Federation No. 40-FZ "On Federal Security Service" dated April 3, 1995, as amended, Article 13(m).
[89] Federal Law of the Russian Federation No. 40-FZ "On Federal Security Service" dated April 3, 1995, as amended, Article 12.
[90] Article 46(2) of the Constitution of the Russian Federation ("Decisions and actions (or inaction) of bodies of state authority and local self-government, public associations and officials may be appealed against in court."). The FSB Law contains a similar rule with respect to FSB decisions. Federal Law of the Russian Federation No. 40-FZ "On Federal Security Service" dated April 3, 1995, as amended, Article 6.
[91] Del Quentin Wilber, *Justice Department to Be More Aggressive in Seeking Encrypted Data*, WALL ST. JOURNAL, Oct. 10, 2017, https://www.wsj.com/articles/justice-department-to-be-more-aggressive-in-seeking-encrypted-data-1507651438.

e. FSB Licensing Regime

i. Kaspersky Lab Requires Licenses from the FSB

One assertion relied upon in support of the BOD is that Kaspersky Lab has obtained certificates and licenses from the FSB, and that such receipt "suggest[s] an unusually close" relationship.[92]

To the contrary, 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. In fact, U.S.-based information technology companies involved in cryptography-related activities operating in Russia are required to obtain the same licenses and certificates from the FSB.

In Russia, the agency responsible for the issuance of domestic activity licenses for technology products with encryption functions and features ("encryption-based products") is a subdivision of the FSB called the Center for Licensing, Certification and Protection of State Secret Information (the "FSB Licensing Center"). The FSB Licensing Center issues local encryption licenses authorizing Russian legal entities to locally distribute encryption-based products, perform technical maintenance, service, and support of such products, as well as provide encryption-based services. U.S. companies engaged in the manufacture and distribution of such products and provision of relevant services typically establish Russian subsidiaries in order to promote local sales and provide relevant services and maintenance of their products to local customers. In order to comply with the licensing requirements, Russian subsidiaries of U.S. and other multi-national companies must have relevant internal activity licenses issued by the FSB.

Recognizing the role of the FSB in granting certificates for certain commercial products, the U.S. Department of the Treasury, Office of Foreign Asset Control ("OFAC") issued General License No. 1 under the Cyber Sanctions Executive Orders which expressly authorized: "[r]equesting, receiving, utilizing, paying for, or dealing in licenses, permits, certifications, or notifications issued or registered by the [FSB] for the importation, distribution, or use of information technology products in the Russian Federation."[93] These activities would otherwise have been prohibited due to the FSB's prior designation pursuant to Executive Order 13757.[94]

In fact, Kaspersky Lab obtains licenses and certifications from all the countries it operates in, including one from NIST, certifying the Company's encryption technologies for businesses as being fully compliant with the Federal Information Processing Standards 140-2.

---

[92] DHS Memorandum, *supra* note 3, at 9.

[93] Office of Foreign Assets Control, U.S. Dep't of Treasury, Cyber General License No. 1: Authorizing Certain Transactions with the Federal Security Service (Feb. 2, 2017), https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber_gl1.pdf.

[94] On December 29, 2016, President Obama issued Executive Order 13757 (amending Executive Order 13694,), and providing for the imposition of sanctions on individuals and entities responsible for "undermining election processes or institutions." Five entities, including the FSB, were accordingly added to OFAC's list of Specially Designated Nationals, https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber2_eo.pdf.

ii. Military Unit Noted on Certain Kaspersky Lab Certificates Does Not Indicate FSB or Military Affiliation

At Section III. D(1) of the DHS Memorandum, the DHS discusses at length two compliance certificates dated 2007 and 2011 issued to Kaspersky Lab. The 2007 certificate states that it is issued to "*military unit 43753 Kaspersky Lab Closed Joint Stock Company*", while the 2011 certificate is issued to "*Kaspersky Lab Closed Joint Stock Company, military unit 43753*."

Based on a DHS review of translations of the certificates, the DHS Memorandum speculates that "[i]n both cases, this language in the certificates suggests that Kaspersky Lab either *is* military unit 43753 or *is part of* military unit 43753."[95] DHS further extrapolates, without firm basis, that these notations are somehow suggestive of concerning connections between Kaspersky Lab and the FSB.

This is not the case. Kaspersky Lab and military unit 43753 ("MU 43753") are two separate organizations with two separate registration numbers.

- Kaspersky Lab is a joint stock company registered under registration number 1027739867473.[96]
- MU 43753 (full name: Federal State Budget-Supported Institution "Military Unit 43753") is a state enterprise registered under registration number 1037739023024.[97]

The real reason for the indication of MU 43753 in Kaspersky Lab's certificates is as follows: MU 43753 is the FSB department responsible for the protection of information. As explained above, Kaspersky Lab makes available some of its products to government customers and therefore on occasion participates in public tenders for that purpose. Products sold to state authorities in Russia must be accompanied by necessary compliance certificates. Thus, the FSB issued the 2007 and 2011 certificates to Kaspersky Lab and also to MU 43753, presumably so that the latter would be aware that Kaspersky Lab had obtained the certificates and was eligible to participate in public tenders. This is not dissimilar to the certification role played by NIST in the U.S. as referenced above.

f. SORM Laws

Russia and other countries have implemented national security legislation designed to regulate surveillance aimed at detecting and preventing terrorism and other criminal activities. In Russia, those laws and tools are applicable to telecom companies and Internet Service Providers ("ISPs") only. Kaspersky Lab does not provide communication services, thus the Company is not subject to these laws or other government tools, including Russia's System of Operational-Investigative Measures ("SORM").

Encrypted Kaspersky Lab customer data may theoretically be intercepted by the FSB using SORM only if such data is transmitted through Russian telecom providers' networks or using internet communications and even then only under specific circumstances described below.

---

[95] DHS Memorandum, *supra* note 3, at 9-10.
[96] *See* Exhibit C, an English-language translation of the extract from the Russian Trade Register for Kaspersky Lab.
[97] *See* Exhibit D, an English-language translation of the extract from the Russian Trade Register for MU 43753.

Such a risk exists with respect to any and all data transferred via telecommunications networks and the internet in Russia.

However, the FSB is only legally permitted to use SORM in a limited number of situations, and each use of SORM technology is subject to court oversight. Law enforcement officers wishing to use this technology must obtain a prior court order in each case when the technology is to be used against a particular person or legal entity.[98] In a limited number of emergency situations, SORM may be used with *post facto* confirmation by a court; but court review is required nonetheless. Such emergency situations include those that may lead to a grave offense or a felony as well as those creating an imminent threat to national security. In such cases, SORM may be used based on the reasonable decision of a head of an investigative authority subject to mandatory notification of a court within 24 hours. Within 48 hours of commencement of SORM use the respective authority must obtain a court order approving SORM use.[99]

g. Other Anti-Virus Software Vendors Have Ties to Foreign Countries

Finally, it is clear that other anti-virus products used by the U.S. Government are supplied by companies that have foreign affiliations or operations. Specifically, BRG reviewed publicly available information regarding six additional anti-virus products, also referenced above, used by the U.S. Government, including, Symantec, McAfee, Trend Micro, Avast, AVG, and ESET.

BRG found that several of the anti-virus software developers are based outside the U.S., including Trend Micro, Avast, and ESET.[100] Even Symantec, a U.S.-headquartered company, publicly acknowledges that it has three significant office locations in China.[101]

In addition, all of the anti-virus companies included in BRG's review indicate in their respective end-user license agreement that they may transmit data to third parties located in other countries.[102] Additionally, BRG found that some of the products reviewed communicate with servers located outside of the U.S.[103] In particular, Avast and ESET communicated with servers located in the Czech Republic and Slovakia, respectively.[104]

VII. OTHER U.S. GOVERNMENT STATEMENTS AND ACTION

At Section III. F of the DHS Memorandum, the DHS cites a series of actions taken, and statements made, by other Government agencies or officials as support for their own action. Contrary to the DHS's assertions, these statements are irrelevant to, and provide no support for, the DHS's own action.

---

[98] U.S. Dep't of State, Country Reports on Human Rights Practices for 2016: Russia (2016), *available at* https://www.state.gov/j/drl/rls/hrrpt/humanrightsreport/index.htm?year=2016&dlid=265466#wrapper.
[99] Federal Law of the Russian Federation No. 144-FZ "On Operational-Investigative Activities" dated Aug. 12, 1995, as amended, Article 8.
[100] *See* BRG Assessment, *supra* note 55, at 20-21.
[101] See BRG Assessment, *supra* note 55, at 21.
[102] *See* BRG Assessment, *supra* note 55, at 21.
[103] *See* BRG Assessment, *supra* note 55, at 21.
[104] *See* BRG Assessment, *supra* note 55, at 21.

In fact, these references are counterproductive and only serve to exacerbate the unwarranted and unsupported actions taken by federal, state, and local agencies including DHS itself against Kaspersky Lab. In the same way that DHS here has referred to the statements and actions of others to support their own actions without considering their underlying basis or context, so others have cited to the BOD, notwithstanding its own lack of basis, to support their own otherwise unsupportable actions. This circular reasoning is self-serving and obscures the reality that no publicly available evidence has been presented to support any of these actions.

a. House Committee on Science, Space and Technology

The DHS Memorandum cites to recent oversight activity by the Committee on Science, Space, and Technology of the U.S. House of Representatives ("Committee"), noting that Committee Chairman Rep. Lamar Smith ("Chairman Smith") "has expressed serious concerns about the Company's products," as further support for DHS's conclusions about the security of Kaspersky Lab's products.[105] In doing so, however, DHS disregards important distinctions between the Committee's exercise of its oversight responsibilities and the sufficiency of the process and analysis required before DHS can appropriately issue a directive such as the BOD.

A congressional committee's exercise of its oversight authority should not be taken as evidence of a public policy risk. All committees of the U.S. House of Representatives are tasked with conducting oversight on subjects and federal agencies within their jurisdiction. In the current instance, the July 27, 2017, letter from Chairman Smith to several federal agencies reflects the Committee's effort to "understand[] the effectiveness of the NIST Framework, and potential vulnerability that exist on federal information systems."[106] A subsequent statement by Chairman Smith indicates that this letter and the Committee's oversight related to Kaspersky Lab is part of its efforts to assess the need to update the NIST Framework, an area squarely within the Committee's jurisdiction.[107]

Citations to concerns expressed by a Member of Congress in the course of oversight activity directed at gathering information about a specific topic and assessing whether legislation on that topic is necessary is not an adequate basis on which to justify the action taken through the BOD. These communications are part of a normal dialogue between Members of Congress and third parties to inquire about areas of interest relevant to the Committee's areas of jurisdiction and cannot be accepted as factual findings or conclusions upon which to legislate. To take such statements out of the context of this larger process does not meet the

---

[105] DHS Memorandum, *supra* note 3, at 15.
[106] Letter from Rep. Lamar Smith, Chairman, U.S. House of Representatives, Committee on Science, Space, and Technology to the Honorable Sonny Purdue, Secretary, U.S. Department of Agriculture (Jul. 27, 2017) (received from Congress, on file with Kaspersky Lab) [hereinafter Letter from Rep. Lamar Smith to Secretary Purdue].
[107] "Cybersecurity breaches are so prevalent today that it is hard to keep track of them. Every news cycle seems to include a new major incident. To address the federal government's cybersecurity weaknesses, the Committee hopes to bring H.R. 1224, the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017, to the House floor for a vote." *Bolstering the Government's Cybersecurity: Assessing the Risk of Kaspersky Lab Products to the Federal Government: Hearing Before the H. Committee on Science, Space, and Technology Subcommittee on Oversight*, 115th Cong. (2017) (statement of Rep. Lamar Smith, Chairman, H. Committee on Science, Space, and Technology), *available at* https://science house.gov/legislation/hearings/bolstering-government-s-cybersecurity-assessing-risk-kaspersky-lab-products.

standards to which DHS should adhere when assessing the need for action analogous to the BOD.

It should be noted that while Chairman Smith states in the July 27, 2017, letter referenced above that he has concerns about Kaspersky Lab's products, he also notes that the allegations giving rise to his concerns have not yet been proven true, recognizing that "*If these widely reported allegations prove true*, then the American public has ample grounds on which to rest their concerns…" (emphasis added).[108]

While Kaspersky Lab takes issue with the assertions made regarding its products and senior executives during the course of the Committee's oversight to date, the process by which the Committee is conducting its oversight, gathering facts to better inform itself through information requests to federal agencies, holding public hearings, and inviting Eugene Kaspersky to testify[109] stands in stark contrast to the absence of any apparent fact-gathering or analysis undertaken by DHS and the lack of any process followed prior to issuing the BOD.

b. May 2017 Senate Intelligence Committee Hearing

The DHS Memorandum also cites to a May 2017 Senate Intelligence Committee hearing at which leaders of several intelligence community agencies were asked a question about Kaspersky Lab products. The single word responses of various officials when asked a leading question by Senator Rubio in a politically charged Senate Intelligence Committee hearing regarding Russian state sponsored cyberthreats to the U.S. is not evidence, much less an adequate substitute for the constitutional obligation DHS owes to Kaspersky in properly considering all evidence with respect to Kaspersky Lab and its products. The witnesses were not required to put forward the factual or technical reasons basis for their conclusions and the hearing itself did include any analysis of the same. Under such circumstances, reliance upon these statements does not comport with the requirements DHS must meet to issue the BOD.

Other, arguably more informed, and better prepared, witnesses discussing Kaspersky Lab in the same forum have come to quite different conclusions. For example, Thomas Rid, a former Professor of Security Studies at King's College London and current Professor of Strategic Studies at the Johns Hopkins University School of Advanced International Studies, testified as follows in a March 30, 2017, Senate Select Committee on Intelligence Hearing titled *Disinformation: A Primer in Russian Active Measures and Influence Campaigns*:

> *"It's important to say that Kaspersky is not an arm of the Russian government if we look at the publicly available evidence. Kaspersky has published information about Russian cyber attacks, cyber intrusion campaigns, digital espionage, about several different Russian campaigns. Name any American company that publishes information about American cyber espionage?"*[110]

---

[108] Letter from Rep. Lamar Smith to Secretary Purdue, *supra* note 106.

[109] Although Eugene Kaspersky accepted an invitation to testify at a hearing the Committee's Subcommittee on Oversight planned to convene, the Subcommittee cancelled the hearing. Kaspersky Lab understands the cancellation was due to a scheduling conflict.

[110] *Disinformation: A Primer in Russian Active Measures and Influence Campaigns: Hearing Before the S. Select Committee on Intelligence*, 115th Cong. (2017) (statement of Thomas Rid, King's College London), *available at* https://www.intelligence.senate.gov/hearings/open-hearing-intelligence-matters-1.

c. General Services Administration

The DHS Memorandum cites the July 11, 2017, action by the General Services Administration ("GSA") to remove Kaspersky Lab products from Schedules 67 and 70 as an example of where "other government officials have expressed concerns with Kaspersky products."[111]

However, it is important to note that GSA's Chief Information Officer, David Shive, confirmed during his testimony before the Subcommittee on Oversight of the House Committee on Science, Space, and, Technology on October 25, 2017, that GSA did not assess or analyze the capabilities of Kaspersky products or conclude that such products pose information security risks to government networks. Mr. Shive explained instead that GSA removed Kaspersky products from the approved list of vendors because there was a problem with how three resellers entered the products onto their own GSA schedules.[112]

Consistent with its channel sales model[113] Kaspersky Lab did not itself have a GSA schedule contract, and the company did not direct any reseller to add its products to their schedule contracts. Therefore, while DHS and other government officials, particularly at the state level, continue to cite the GSA action as evidence that Kaspersky products pose information security risks to government networks, GSA itself has acknowledged that it took action for reasons unrelated to the Company.

d. State and Local Action

The federal Government's actions have caused further collateral harm to Kaspersky Lab by inducing a number of States to follow suit in prohibiting their own State and local agencies from using Kaspersky Lab products. The actions of those State and local authorities (taken purely in deference to the federal actions) does not, in turn, validate or add any weight after the fact to the previously initiated actions by the federal government including through the BOD.

Kaspersky Lab has a number of SLED customers that, as a result of these state directives, are required or are otherwise strongly pressured to discontinue their use of Kaspersky Lab software and solutions.

As DHS alludes to,[114] on July 12, 2017, the California Department of General Services, Procurement Division and the California Department of Technology, Statewide Technology Procurement Division, issued Bulletin # P-09-17, which required "all State Departments to immediately discontinue the use of Kaspersky Labs cybersecurity and information

---

[111] DHS Memorandum, *supra* note 3, at 14.
[112] *Bolstering the Government's Cybersecurity: Assessing the Risk of Kaspersky Lab Products to the Federal Government: Hearing Before the H. Committee on Science, Space, and Technology Subcommittee on Oversight*, 115th Cong. (2017) (statement of David Shive, U.S. General Services Administration), *available at* https://science house.gov/legislation/hearings/bolstering-government-s-cybersecurity-assessing-risk-kaspersky-lab-products.
[113] *See* discussion *supra* at Section III.d.
[114] DHS Memorandum, *supra* note 3, at 15.

technology products and suspend all procurement activities of these products until further notice."[115]

Similarly and immediately following the issuance of the BOD, on September 15, 2017, the New York Office of General Services issued CL # 843, advising state departments to contact their IT departments "to commence a review of purchases and contracts for software and services to determine their exposure to Kaspersky Lab products and service" and, if Kaspersky Lab products are installed or a vendor offers Kaspersky Lab products, that the departments "consider whether the concerns raised by the federal government necessitate further action."[116]

On October 25, 2017, the Chief Information Officer of the University of California issued a memorandum to UC Chief Information Officers, announcing a system-wide moratorium on the purchase or deployment of all Kaspersky Lab technologies, requiring locations to submit six-month plans to stop using Kaspersky-branded technologies and eighteen-month plans to remove technologies with Kaspersky-embedded code from their environments.[117] On October 30, 2017, the Texas Education Agency issued a Cyber Alert titled "DHS Issues Binding Operational Directive on Kaspersky Products" recommending that ESCs and LEAs follow the guidance in the federal directive.[118]

As noted above, these reciprocal actions are not evidence of any underlying support or evidence for any of these agencies actions individually, or for all of them collectively.

VIII. BOD RAISES SIGNIFICANT U.S. CONSTITUTIONAL CONCERNS AND FAILS TO PROVIDE ADEQUATE ADMINISTRATIVE PROCESS

Issuing and implementing the BOD with nearly wholesale reliance on public news articles containing self-serving, unverified, and even anonymous statements, without any semblance of a process that allows for the right to be heard, much less the opportunity to confront the evidence used to substantiate such action, results in a clear violation of Kaspersky Lab's rights under both the Due Process and Equal Protection Clauses of the Fifth Amendment. These actions are also clearly arbitrary, capricious, and an abuse of discretion giving rise to challenge under the Administrative Procedure Act.

---

[115] California Department of General Services, Procurement Division and California Department of Technology, Statewide Technology Procurement Division, *Bulletin*, # P-09-17, *Re: Kaspersky Anti-Virus Software*, July 18, 2017, https://www.documents.dgs.ca.gov/pd/delegations/broadcastbulletins/2017/pac071817_P-09-17.pdf.

[116] New York State Office of General Services, *General Information Bulletin*, CL # 84 *Subject: Kaspersky Lab Sofware and Cybersecurity Services,* Sept. 15, 2017, https://www.ogs.ny.gov/purchase/spg/pdfdocs/CL843.pdf.

[117] University of California, Executive Vice President – Chief Operating Officer, *Letter to CRE's & CIO's*, Oct. 25, 2017, http://news.ucmerced.edu/sites/news.ucmerced.edu/files/documents/kaspersky_memo_w_attachments_10-25-17.pdf.

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

a. DHS's Professed "Administrative Process" Following The Issuance of the BOD Violates Kaspersky Lab's Due Process Rights

As part of the BOD, DHS also announced that it would be making available a yet to be specified administrative process "to inform [DHS] decision making" as to Kaspersky Lab and any other entity which claims that its commercial interests will be directly impacted by the BOD.[119] Under that professed process, which was only articulated in the Federal Register on September 19, 2017,[120] the date set for a response by Kaspersky Lab and any other affected parties is November 3, 2017, which has subsequently been extended to November 10, 2017.[121] Following receipt of this response, "the Secretary's decision will be communicated to the entity in writing by December 13, 2017."[122] This will occur after action has already been required to have been taken by the federal agencies subject to the BOD. In addition, the "[t]he Secretary reserves the right to extend the timelines identified above."[123]

DHS has violated Kaspersky Lab's rights under the Due Process Clause of the Fifth Amendment by offering a deficient "administrative process" that deprives Kaspersky Lab of a constitutionally protected liberty interest without due process of law.

"Due process is flexible and calls for such procedural protections as the particular situation demands,"[124] but fundamentally requires "the opportunity to be heard at a meaningful time and in a meaningful manner."[125] Procedures are not meaningful unless they offer "an opportunity to effectively be heard"[126] and the courts have consistently held that notice of the proposed official action, access to the unclassified evidence supporting that action, and an opportunity to rebut the evidence are essential elements of due process.[127]

In addition, the courts have also made clear that such process must be provided *before* action is taken to deprive entities of their property or liberty interests. For example, in *People's Mojahedin Organization of Iran v. Department of State*, a case concerning the PMOI's designation by the State Department as a foreign terrorist organization, the D.C. Circuit held that "due process requires that the PMOI be notified of the unclassified material on which the

---

[119] DHS Letter to Eugene Kaspersky, 1 (Sept. 13, 2017).
[120] National Protection and Programs Directorate; Notification of Issuance of Binding Operational Directive 17–01 and Establishment of Procedures for Responses, 82 Fed. Reg. 180, 43783, 43784 (Sept. 19, 2017).
[121] *See* Exhibit E, Email Correspondence with Daniel Sutherland.
[122] *Id.*
[123] *Id.*
[124] *Morrissey v. Brewer*, 408 U.S. 471, 481 (1972).
[125] *Mathews v. Eldridge*, 424 U.S. 319, 333 (1976) (quoting *Armstrong v. Manzo*, 380 U. S. 545, 552 (1965)).
[126] *Nat'l Council of Resistance of Iran v. Dep't of State* (*NCRI*), 251 F.3d 192, 208 (D.C. Cir. 2001).
[127] *See Greene v. McElroy*, 360 U.S. 474, 496 (1956) (Holding that it is an "immutable" principle that "where governmental action seriously injures an individual, and the reasonableness of the action depends on fact findings, the evidence used to prove the Government's case must be disclosed to the individual so that he has an opportunity to show that it is untrue"); *NCRI*, *supra* note 126, at 208 ("[T]hose procedures which have been held to satisfy the Due Process Clause have 'included notice of the action sought,' along with the opportunity to effectively be heard."); *Gray Panthers v. Schweiker*, 652 F.2d 146, 165 (D.C. Cir. 1980) (holding that "adequate notice of why the benefit is being denied and a genuine opportunity to explain why it should not be" is a "core requiremen[t] of due process.")

Secretary proposes to rely and an opportunity to respond to that material *before* its [terrorism] redesignation."[128]

Similarly, in *Ralls Corporation vs. Committee on Foreign Investment in the United States*, a case concerning whether the Ralls Corporation had received adequate process during a national security review of a proposed transaction by CFIUS prior to a Presidential order divesting it of a property interest, the D.C. Circuit held that Ralls should have received this same set of procedural protections "*before* the Presidential Order prohibit[ing] the transaction."[129]

The BOD provides no equivalently sufficient due process protection. While access to the DHS Memorandum--an internal 21 page summary drafted in support of the BOD--has been provided, there was no effective opportunity to test or rebut the "evidence" contained therein before action was taken, and therefore there has been no "opportunity to effectively be heard."[130] As referenced above, the "process" purportedly provided by the BOD lays out a timeline in which federal agencies will begin removal of Kaspersky-branded products from their information systems by December 12, 2017, and the Secretary of Homeland Security is only required to finish considering this response a day later, on December 13, 2017. The Secretary also reserves the right to freely extend the period of consideration beyond December 13, 2017. The BOD's "process" therefore violates Kaspersky Lab's due process rights and runs counter to the consistent line of cases establishing that these rights must be provided before any deprivation of a property or liberty interest occurs.

Although the BOD's 30-60-90 day structure gives the impression that the harm is not immediate, in reality, the BOD effectuates an immediate and complete prospective debarment of Kaspersky Lab from government business. No affected federal agency is able to purchase Kaspersky Lab products because, from the moment of issuance, the BOD orders the discontinuation and removal of those products.

Kaspersky has a claim for denial of procedural due process because "(1) the government deprived [it] of a liberty … interest to which [it] had a legitimate claim of entitlement, and (2) … the procedures attendant upon that deprivation were constitutionally insufficient."[131]

(i) Deprivation of Liberty Interest

It is long established that "a person's 'right to ... follow a chosen profession free from unreasonable governmental interference comes within the 'liberty' ... concept[] of the Fifth Amendment.'"[132] "[T]his liberty concept protects corporations as well as individuals…."[133] So, for example, "debarring a corporation from government contract bidding constitutes a deprivation of liberty that triggers the procedural guarantees of the Due Process Clause."[134] In

[128] *People's Mojahedin Organization of Iran v. Department of State* (*PMOI II*), 613 F.3d 220, 228 (D.C. Cir. 2010) (emphasis added).
[129] *Ralls Corp. v. Comm. on Foreign Inv. in the U.S* ., 758 F.3d 296, 320 (D.C. Cir. 2014) (emphasis added).
[130] *NCRI*, *supra* note 126, at 208.
[131] *Jefferson v. Harris*, 170 F. Supp. 3d 194, 204 (D.D.C. 2016) (internal quotations omitted; alterations omitted).
[132] *Trifax Corp. v. District of Columbia*, 314 F. 3d 641, 643 (D.C. Cir. 2003) (quoting *Greene v. McElroy*, *supra* note 127, at 492).
[133] *Id*.
[134] *Id.*

fact, "[a]ll reputation-based [procedural-due-process] claims depend on some deprivation of liberty—in general terms, a constitutionally protected interest in one's good name or in being able to pursue one's chosen profession—without procedures that were constitutionally sufficient."[135] "[S]uch actions are not monolithic"—rather, in the D.C. Circuit, "two independent [albeit not mutually exclusive] theories for how such deprivations occur have crystallized."[136] Both support claims by Kaspersky Lab.

First, Kaspersky Lab has "what is known as a 'stigma-plus'" claim.[137] This claim is based "on a continuing stigma or disability arising from official *action*."[138] Under this theory, a liberty interest is infringed when '"preclusion [from government contracting] is either sufficiently formal *or* sufficiently broad.'"[139] Here, Kaspersky Lab has claims on both formal debarment and alternatively a "broad preclusion" that "seriously affected, if not destroyed, [Kaspersky Lab's] ability to obtain… [contracts] in [its] field."[140]

DHS's statements also support a so-called "reputation-plus" claim.[141] That claim is predicated on "defamation that is '*accompanied* by a discharge from government employment or at least a demotion or rank in pay."[142] While "[t]his theory makes the termination actionable only where the terminating employer has disseminated the reasons for the termination and such dissemination is defamatory"—that is what has happened here as DHS effectively terminated Kaspersky Lab as a government contractor while simultaneously broadcasting to the world insufficient, uncorroborated, and self-serving reasons for that termination.[143]

(ii) Constitutionally Insufficient Procedures

This deprivation—on either a stigma-plus or reputation-plus theory—violated Kaspersky Lab's Fifth Amendment rights because the BOD afforded no pre-deprivation process. As explained above, without notice, the BOD effectuated an immediate debarment and preclusion of Kaspersky Lab upon issuance. Pre-deprivation process clearly was required here under the three-factor test set forth in *Mathews v. Eldridge*, which weighs (1) "the private interest . . . affected by the official action;" (2) "the risk of an erroneous deprivation of such interest through the procedures used;" and (3) "the government's interest, including the function involved and the fiscal and administrative burdens that . . . additional or substitute procedural requirement would entail."[144]

---

[135] *Liff v. Office of the Inspector General for the U.S. Department of Labor*, 2016 U.S. Dist. LEXIS 153979, *20 (D.D.C. 2016)
[136] *Id.*
[137] *Jefferson*, 170 F. Supp. 3d at 205.
[138] *Id.* (internal quotations omitted; emphasis in original).
[139] *Trifax*, 314 F. 3d at 644 (quoting *Taylor v. Resolution Trust Corp.*, 56 F.3d 1497, 1505 (D.C. Cir. 1995)) (emphasis added).
[140] *Id.* (internal quotations omitted; alterations in original). *See also Liff v. Office of the Inspector General for the U.S. Department of Labor*, 156 F. Supp. 3d 1, 21 (D.D.C. 2016) (citing *Kartseva v. Dep't of State*, 37 F.3d 1524, 1527 (D.C. Cir. 1994)) (explaining that government contractor suffers deprivation when broadly precluded).
[141] *Liff,* 2016 U.S. Dist. LEXIS 153979 at *20 (D.D.C. 2016).
[142] *Id*. at *20 (quoting *O'Donnell v. Barry*, 148 F.3d 1126, 1140 (D.C. Cir. 1998)) (emphasis in original).
[143] *Id*. at *20-21 (internal quotation omitted).
[144] *Mathews*, 424 U.S. 319, 335 (1976). *See, e.g., NCRI*, *supra* note 126, at 205-208; *KindHearts for Charitable Humanitarian Dev., Inc., v. Geithner*, 647 F. Supp. 2d 857, 901 (N.D. Ohio 2009).

Under the first *Matthews* 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 generally. Under the second factor, DHS's failure to provide adequate and timely notice creates a substantial risk of wrongful deprivation. Finally, under the third factor, DHS has failed to demonstrate how prior notice to Kaspersky Lab would have interfered with its goals of eliminating the alleged "information risks" or relatedly why it failed to consider potential mitigation when such a consideration may have helped guard against the BOD being overbroad or more severe than necessary.

Indeed, as the D.C. Circuit explained in *National Council of Resistance of Iran v. Department of State*, with respect to the designation of a foreign terrorist organization by the State Department, "It is simply not the case . . . that the Secretary has shown how affording the organizations whatever due process they are entitled to before their designation as foreign terrorist organizations and the resulting deprivation of right would interfere with the Secretary's duty to carry out foreign policy."[145] In that case, 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:

> 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.[146]

The same is true here. This is not a case where a pre-deprivation process would "cripple" the underlying statute—in contrast to, for example, "providing notice before blocking the assets of international narcotic traffickers would create a substantial risk of asset flight."[147] Thus, the D.C. Circuit has observed "[t]hough the Due Process Clause generally requires the Government to afford individuals notice and an opportunity to be heard *before* depriving them of their property, there are 'extraordinary situations where some valid governmental interest is at stake that justifies postponing the hearing until after the event.'"[148]

But nowhere does the BOD, or the supporting DHS Memorandum even suggest 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. To the contrary, DHS provides *three months* for affected agencies to "begin to implement their plan of action."[149] 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.

---

[145] *NCRI*, *supra* note 126, at 207-208.
[146] *Id. See also PMOI II*, *supra* note 128, at 227.
[147] *Zevallos v Obama*, 793 F.3d 106, 116 (D.C. Cir. 2015).
[148] *Id* (quoting *Boddie v. Connecticut*, 401 U.S. 371, 379 (1971)) (emphasis added; internal quotations omitted). *See also, e.g.*, *Cleanmaster Industries, Inc. v. Shewry*, 491 F. Supp. 2d 937 (C.D. Cal. 2007) ("The Department has not provided evidence of any circumstances that would necessitate the immediate suspension of the plaintiff from the Medi-Cal program, and the concomitant publication of that debarment . . . , prior to providing the plaintiff with a name-clearing hearing.")
[149] BOD, *supra* note 1, at 3.

Indeed, DHS had ample opportunity to engage with Kaspersky Lab prior to the issuance of the BOD. Kaspersky Lab wrote to DHS on July 18, 2017,[150] with an offer to provide any information or assistance with regard to any investigation involving the Company, its operations, or its products. At that time, Kaspersky Lab was unaware of what action, if any, DHS was contemplating. In response to Kaspersky Lab, nearly a month later, on August 14, 2017, DHS acknowledged the Company's letter and its offer of assistance, and indicted that DHS "*will be in touch again shortly.*" (emphasis added).[151] No further communication was received prior to the issuance of the BOD. Even following the issuance of the BOD, DHS has repeatedly declined the requests of the Company and its counsel to engage in order to present the Company's position, address DHS's concerns, and discuss any potential options for mitigation.[152]

By way of comparison, an example of an approach in which entities are provided meaningful process can be found in the Federal Acquisition Regulations ("FAR"), which prescribe the policies and procedures governing the debarment and suspension of contractors for cause by federal agencies.[153] The FAR usefully illustrates how this process and the appurtenant procedural protections are typically provided in the debarment context. In that process, debarring officials must afford contractors a formal notice of proposed suspension and/or debarment which must include: (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) the procedures that will govern the agency's decision-making process, and (4) the effects of proposed and actual debarment.[154] Crucially, the debarring official's decision may only be made within 30 working days *after* receipt of information and argument from the contractor.[155] This final protection 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.

Of particular note, the DHS Memorandum 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 – finding that unlike a FAR debarment, 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.[156] And so, paradoxically, even though it is more thorough in depriving Kaspersky Lab of its property 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 government contracts.

[150] *See* Exhibit F, Kaspersky Lab Letter to DHS (July 18, 2017).
[151] *See* Exhibit G, DHS Response to Kaspersky Lab (Aug. 14, 2017).
[152] *See* Exhibit E, Email Correspondence with Daniel Sutherland.
[153] 48 C.F.R. Part 9.400(a)(1).
[154] 48 C.F.R. Part 9.406-3(c).
[155] 48 C.F.R. Part 9.406-3(d)(1).
[156] DHS Memorandum, *supra* note 3, at 4.

b. Through the BOD, DHS Has Violated Kaspersky Lab's Constitutional Right To Equal Protection

DHS also has violated Kaspersky Lab's rights under the Equal Protection Clause of the Fifth Amendment by singularly applying FISMA and the BOD solely to Kaspersky Lab, and not to other similarly-situated companies which also develop and sell anti-virus software to the U.S. Government. This conduct establishes the essential elements of a "class of one" equal protection claim, based on the U.S. Supreme Court's decision in *Village of Willowbrook v. Olech*: intentional, disparate treatment of similarly-situated parties—without a rational basis.[157] Specifically, "[t]o state a claim for 'class of one' equal protection, at the very least, a party must allege that (1) he was treated differently from others similarly situated, (2) it was done so intentionally, and (3) there was no rational basis for the difference in treatment."[158] These elements are satisfied here.

Kaspersky Lab is similarly situated to other anti-virus software manufacturers—*i.e.*, its competitors—including Avast (Czech Republic), AVG Technologies (Czech Republic), ESET (Slovakia), and Trend Micro (Tokyo). Each of these companies, like Kaspersky Lab, develop and sell similar anti-virus software to the federal government.[159] Each of these companies are headquartered in foreign countries, offer products that operate with elevated levels of system privileges, send anti-virus definition updates over international borders, and include broad allowances for data collection via networks similar to KSN. Yet DHS has singled out Kaspersky Lab. DHS's dissimilar treatment is clearly intentional and is designed to exclude the Company from the U.S. market.

DHS has demonstrated no rational basis for applying FISMA and the BOD exclusively to Kaspersky Lab because the use of other foreign anti-virus services present virtually all of same risks DHS has associated with Kaspersky Lab products and services. Nor does Kaspersky Lab having its headquarters in Russia present unique risks. Per the BRG Assessment, one of Kaspersky Lab's competitors, Avast, includes a security product in its anti-virus offering that maintains servers in China and Russia. There is plainly no rational basis for DHS's differential treatment of Kaspersky Lab products and those of its other foreign competitors.

Further, it is clear that the intent of the BOD, and the U.S. Government more generally, is to unfairly interrupt Kaspersky Lab's commercial interests. Recent public statements, often politically or commercially motivated and thin on facts, have, for example, led several big box retailers to remove Kaspersky Lab products from their shelves and suspend their long-standing partnerships with Kaspersky Lab. Several of these retailers, which have provided a steady stream of both new customers and consumer product subscription renewals to

---

[157] *Vill. of Willowbrook v. Olech*, 528 U.S. 562, 564 (2000) ("Our cases have recognized successful equal protection claims brought by a 'class of one,' where the plaintiff alleges that she has been intentionally treated differently from others similarly situated and that there is no rational basis for the difference in treatment.") *See also 3883 Connecticut LLC v. District of Columbia*, 336 F.3d 1068, 1075 ("[T]here are "two essential elements of [a] 'class of one' equal protection claim: (1) disparate treatment of similarly situated parties (2) on no rational basis.")

[158] *Galicki v. New Jersey*, 2016 U.S. Dist. LEXIS 126076, *50 (D.N.J. Sept. 15, 2016) (class-of-one claims adequately pleaded against Governor Chris Christie and others based on George Washington Bridge lane closure (*i.e.*, 'Bridgegate')) (internal quotations omitted).

[159] *See* BRG Assessment, *infra* note 55, at 9-20.

Kaspersky Lab over the years, went even further and, upon removing Kaspersky Lab products encouraged and otherwise incentivized existing Kaspersky Lab software customers (current license holders) to "switch" to the software of one of Kaspersky Lab's competitors in the market.

As a result of these actions, Kaspersky Lab's 2017 Q3 retail sales have fallen 37 percent as compared to the same period in 2016. Similarly, the amount of business Kaspersky Lab derived from new online sales customers in the month of October 2017, the month immediately following the issuance of the BOD, declined 30 percent versus the same period in 2016.

At present, Kaspersky Lab is receiving and processing an unprecedented volume of product return and early termination requests, as a result of the U.S. Government's actions (which customers specifically refer to when stating the reason for their return), which will certainly cause the Company's U.S. results to decrease significantly.

Kaspersky Lab's 2017 Q3 U.S. bookings have fallen by over 15 percent since the previous quarter and are 16 percent lower than the results for same quarter in the previous year (2016 Q3), demonstrating the immediate, significant, and detrimental effect of the U.S. Government's actions, including the issuance of the BOD.

Making no effort to disguise the broader intent of this action, 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,[160] in response to a question at a public forum as to how and to what extent consumers should be informed as to the nature of any risk posed by Kaspersky Lab products, while continuing to conceal the specific nature of the risk from the public, stated "…when [DHS] makes a pretty bold statement like issuing the Kaspersky Lab binding operational directive I think that's a fairly strong signal [to consumers]."[161]

The potential implications of this action by DHS go far beyond extinguishing the limited amount of federal government business in which Kaspersky Lab has indirectly profited from as summarized above.[162] The impact will extend to and is already being felt in the Company's commercial business. Recent comments indicate DHS is well aware of and actively supports such adverse impacts of its action. Thus, the BOD not only deliberately deprives Kaspersky Lab of its liberty to engage in its chosen business in violation of the Fifth Amendment's Due Process Clause, but also violates Kaspersky Lab's Fifth Amendment Equal Protection rights.

c. DHS Action Through The BOD is Arbitrary, Capricious, and an Abuse Of Discretion

The Administrative Procedure Act provides for judicial review of agency action.[163] If review is available, courts may hold unlawful and set aside agency action, findings, and conclusions

[160] DHS Memorandum, *supra* note 3, at 1.
[161] *See* Aspen Institute, *Is the US Losing the Cyber Battle?* (Oct. 31, 2017), https://www.aspeninstitute.org/events/us-losing-cyber-battle/.
[162] *See* discussion *infra* at Section III(d).
[163] 5 U.S.C. § 702 ("A person suffering legal wrong because of agency action, or adversely affected or aggrieved by agency action within the meaning of a relevant statute, is entitled to judicial review thereof.")

that are, among other potential deficiencies, contrary to constitutional right, power, privilege, or immunity[164] or arbitrary, capricious, an abuse of discretion or otherwise not in accordance with the law.[165]

As discussed in Section VIII(a), the process offered by DHS has the effect of depriving Kaspersky Lab of a constitutionally protected liberty interest without due process of law in violation of the Fifth Amendment's Due Process Clause. As discussed in Section VIII(b), DHS has also violated Kaspersky Lab's Fifth Amendment Equal Protection rights. These constitutional violations can not survive APA scrutiny.

A reviewing court may also hold unlawful and set aside agency actions that are arbitrary, capricious, an abuse of discretion or otherwise not in accordance with the law.[166] While a court reviewing agency findings under the arbitrary and capricious standard may not "substitute its judgment for that of the agency,"[167] it must ensure that the agency has "articulat[ed] a satisfactory explanation for its action including a 'rational connection between the facts found and the choice made.'"[168] Under this standard, agency decisions not supported by "substantial evidence" may be reversed.[169]

The BOD is such an agency decision. The DHS Memorandum does not identify any evidence of any malicious cyber conduct on the part of Kaspersky Lab, or even allege that Kaspersky Lab has engaged in any such malicious cyber conduct. Nor does it identify any technical concerns that are unique to Kaspersky Lab products. DHS's arguments and concerns are based entirely on speculation and innuendo, relying on the statements from anonymous sources made to newspapers, self-interested public statements by competitors and security professionals who do not have knowledge of the design of Kaspersky Lab products, and statements by government officials who have been subjected to political pressure to make such statements with no indication or support that they or their staff has closely examined the products they were questioned about.

The BOD is, instead, based on a series of perceived risks derived from (i) DHS's understanding of the functionality of anti-virus software, (ii) the fact that Kaspersky Lab is a Russian company subject to Russian legal provisions that could require Kaspersky Lab to provide certain information technology assistance to the FSB, and (iii) the assertion that, because Kaspersky Lab requires certain licenses and certifications from the FSB to engage in encryption regulated activities in Russia, it may be vulnerable to "leverage" by the Russian Government.[170]

---

[164] *Id.* § 706(2)(B).
[165] *Id.* § 706(2)(A).
[166] 5 U.S.C. § 706(2)(A).
[167] *Motor Vehicle Mfrs. Ass'n of the U.S. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983).
[168] *Id.* at 43 (quoting *Burlington Truck Lines, Inc. v. United States*, 371 U.S. 156, 168 (1962)).
[169] *J.A. Jones Mgmt. Servs. v. FAA,* 225 F.3d 761, 764 (D.C. Cir. 2000) (quoting *Kisser v. Cisneros,* 14 F.3d 615, 619 (D.C. Cir. 1994)) ("Under this standard, we 'may reverse only if the agency's decision is not supported by substantial evidence, or the agency has made a clear error in judgment.'")
[170] DHS Memorandum, *supra* note 3, at 16. Kaspersky Lab's response to each of these issues is set out at Sections V, and VI above.

Courts may appropriately consider the record as a whole and consider "whatever in the record fairly detracts from [the] weight" of the agency's proffered evidence.[171] Other professionals and governmental organizations have already reached different conclusions based on the publicly available evidence. For example, on October 11, 2017, Germany's BSI federal cyber agency indicated that it had "… no plans to warn against the use of Kaspersky Lab products since the BSI has no evidence for misconduct by the Company or weaknesses in its software."[172]

On October 12, 2017, the Department of Prime Minister and Cabinet of Australia confirmed that the Australian Government is not following the U.S. Government's lead in banning Kaspersky Lab products despite being "in constant engagement with our Five Eyes security partners on this matter," referring to the Five Eyes intelligence sharing network which includes its four most trusted Western allies: the U.S., the U.K., Canada and New Zealand.[173]

On the same day, INTERPOL announced that it had signed a new threat intelligence exchange agreement with Kaspersky Lab, stating "Since the first agreement between the two organizations was signed in 2014, Kaspersky Lab experts have regularly cooperated with INTERPOL to share fresh cyberthreat discoveries with police in its member countries." The statement went on to cite Kaspersky Lab's participation in an INTERPOL-led cybercrime operation, which identified nearly 9,000 botnet command and control servers and hundreds of compromised websites, including government portals, across the ASEAN region as well as Kaspersky Lab's previous cooperation in a global operation coordinated by the INTERPOL Global Complex for Innovation ("IGCI") in Singapore to disrupt the Simda criminal botnet – a network of more than 770,000 infected PCs around the world.[174]

Even some of those sources on which DHS seeks to base its own decision, have now openly criticized the actions being taken by DHS against Kaspersky Lab. For example Jeffrey Carr, founder and CEO of Taia Global, who's 2012 report "*Russian Laws and Regulations: Implications for Kaspersky Labs [sic]*"[175] is cited extensively in the DHS Memorandum wrote (in his personal capacity) a blog post titled *U.S. Government Bans Kaspersky Lab Without Cause,* on September 14, 2017, in direct response to news of the BOD, saying:

> "The ban is both malicious and ignorant. It's ignorant because Kaspersky Lab has data on malware coming out of Russia and the CIS that no one else has. By banning their products, the U.S. government has blocked its best source of cyber threat intelligence coming out of a region where it desperately needs it.

---

[171] *Town of Barnstable*, 740 F.3d 681, 687 (quoting *Universal Camera Corp. v. NLRB*, 340 U.S. 474, 488 (1951)).
[172] *See* Reuters, *Germany: 'No evidence' Kaspersky software used by Russians for hacks*, REUTERS, Oct. 11, 2017, https://www reuters.com/article/us-usa-security-kaspersky-germany/germany-no-evidence-kaspersky-software-used-by-russians-for-hacks-idUSKBN1CG284 ("Germany's BSI federal cyber agency said on Wednesday it had no evidence to back media reports that Russian hackers used Kaspersky Lab antivirus software to spy on U.S. authorities.")
[173] Jackson Gothe-Snape, *No Aussie ban for Russian anti-virus firm Kaspersky Lab, but it does have new lobbyists,* AUSTRALIA BROADCASTING CORPORATION, Oct. 12, 2017, http://www.abc net.au/news/2017-10-12/no-ban-for-lobbyist-backed-russian-anti-virus-company/9042246.
[174] Interpol, *INTERPOL and Kaspersky Lab sign new threat intelligence exchange agreement* (Oct. 12, 2017), https://www.interpol.int/News-and-media/News/2017/N2017-137.
[175] *See* DHS Memorandum, supra note 3 at Exhibit 17.

It's malicious because there's no basis in fact for the charge that Kaspersky products have a backdoor."[176]

Finally, we note that in Section VI of the DHS Memorandum ("Analysis of Available Contrary Evidence"), DHS purports to consider, in a cursory fashion, certain contrary evidence relevant to the recommendation to issue the BOD. But none of these statements were made in the context of, or directly in response to, the BOD. Rather, many of those statements were made under different circumstances and are either irrelevant or taken out of context and have been self-selected and arranged by DHS in an attempt to bolster its own position. These statements (and particularly DHS's representation of them) should not, and must not, be considered Kaspersky Lab's response to the BOD, nor are they necessarily responsive to the issues at hand. They cannot be considered any substitute for Kaspersky Lab's constitutional right to be heard.

Taken together, the forgoing demonstrates that 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. The full record simply does not amount to "substantial evidence"[177] and DHS's BOD should therefore be rescinded, less it be invalidated under the APA as an arbitrary and capricious abuse of agency discretion.[178]

IX. FOIA NOTICE

Finally, while we believe that this submission is exempt from disclosure under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552(b)(4), we request that your office provide us with written notification of any request under FOIA for release of the information contained herein. To the extent that this submission is reviewed or retained by other agencies of the U.S. Government, we request that it be protected from disclosure by those agencies pursuant to FOIA. If a decision is made to release this material, whether pursuant to a FOIA request or for any other reason, we request that we be provided with a ten-day advance written notice to the undersigned of any proposed release.

Respectfully Yours,

Ryan Fayhee
Partner
+1 202 452 7024
ryan.fayhee@bakermckenzie.com

[176] J. Carr *U.S. Government Bans Kaspersky Lab Without Cause* https://medium.com/@jeffreycarr/u-s-government-bans-kaspersky-lab-without-cause-b59cbb50ed56.
[177] *See supra* note 169.
[178] *J.A. Jones Mgmt. Servs. v. FAA*, *supra* note 169, at 255; 44 U.S.C. § 3552(b)(1)(A).

Encls.

Exhibit List

Exhibit A – KGSS Cyber Threat Intelligence Product Catalogue
Exhibit B – BRG Assessment
Exhibit C – Russian Trade Register for Kaspersky Lab
Exhibit D – Russian Trade Register for MU 43753
Exhibit E – Email Correspondence with Daniel Sutherland
Exhibit F – Kaspersky Lab Letter to DHS 7.18.17
Exhibit G – DHS Response to Kaspersky Lab 8.14.17