Office of Cybersecurity and Communications
National Protection and Programs Directorate
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

December 4, 2017

INFORMATION

MEMORANDUM FOR THE ACTING SECRETARY

THROUGH: Christopher C. Krebs
Senior Official Performing the Duties of the Under Secretary

FROM: Jeanette Manfra
Assistant Secretary

SUBJECT: **Final Decision on Binding Operational Directive 17-01, Removal of Kaspersky-Branded Products**

I. PURPOSE

This memorandum summarizes information obtained by the Department since you issued Binding Operational Directive ("BOD") 17-01 on September 13, 2017. This includes information and arguments submitted by Kaspersky Lab pursuant to the administrative process made available by the Department (the "Kaspersky Submission");[1] information submitted by agencies as required by the BOD; an analysis of relevant portions of Russian law prepared by Professor Peter Maggs of the University of Illinois College of Law (the "Maggs Report");[2] a supplemental information security risk assessment prepared by the NCCIC (the "NCCIC Supplemental Assessment");[3] and a section of the National Defense Authorization Act for FY 2018 ("NDAA") that imposes a government-wide ban on the use of Kaspersky products.[4]

Based on the totality of the evidence, including evidence in the September 1, 2017 Information Memorandum and its exhibits (the "Information Memorandum"),[5] your September 13, 2017 Decision Memorandum (the "Decision Memorandum"), the Kaspersky Submission, and other information and developments since issuance of the BOD, I recommend that you issue a Final

---

[1] The Kaspersky Submission consists of a *Kaspersky Lab Request for Department of Homeland Security to Initiate Review of Binding Operational Directive – 17-01*, submitted by counsel for Kaspersky at Baker & McKenzie LLP, and seven exhibits (Exhibits A-G). The full Kaspersky Submission is provided as Attachment D to the Action memorandum to which this Information memorandum is attached. References below to the "Kaspersky Submission" with page numbers refer to pages in the *Kaspersky Lab Request* submitted by Baker & McKenzie. References to the BRG Assessment refer to Exhibit B to the *Kaspersky Lab Request*.

[2] The Maggs Report is provided as Exhibit 1.

[3] The NCCIC Supplemental Assessment is provided as Exhibit 2.

[4] This section of the NDAA is provided as Exhibit 3.

[5] The Information Memorandum and its first exhibit, the NCCIC Assessment discussed below, are attached as Exhibit 4 and Exhibit 4.A, respectively.

information and developments since issuance of the BOD, I recommend that you issue a Final Decision memorandum (the "Final Decision") that maintains BOD 17-01 without modification. I also recommend that you transmit a letter to Kaspersky enclosing the Final Decision, this memorandum, and its exhibits, including the NCCIC Supplemental Assessment and the Maggs Report.

This memorandum proceeds as follows. Section II provides context for these recommendations, including the standard for issuing BODs and the rationale for issuing BOD 17-01. Section II.A explains four mechanisms by which DHS obtained information since issuance of BOD 17-01: the Kaspersky Submission; other public statements by Kaspersky; reports and other communications from federal agencies; and the Maggs Report. Section III addresses the Kaspersky Submission in detail, starting with Kaspersky responses to specific concerns in the Information Memorandum and Decision Memorandum (Section III.A) followed by additional information and arguments presented by Kaspersky (Section III.B). Section IV analyzes the record and recommends issuance of the Final Decision and transmission to Kaspersky.

II. CONTEXT AND TIMELINESS

BOD 17-01 requires all federal executive branch departments and agencies to (1) identify the use or presence of "Kaspersky-branded products"[6] on all federal information systems within 30 days of BOD issuance (*i.e.*, by October 13); (2) develop and provide to DHS a detailed plan of action to remove and discontinue present and future use of all Kaspersky-branded products within 60 days of BOD issuance (*i.e.*, by November 12);[7] and (3) begin to implement the plan of action at 90 days after BOD issuance (*i.e.*, December 12),[8] unless directed otherwise by DHS in light of new information obtained by DHS, including but not limited to new information submitted by Kaspersky.

The Secretary of Homeland Security is authorized to issue BODs, in consultation with the Director of the Office of Management and Budget, for the purpose of safeguarding federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk.[9] I recommended issuing the BOD in the Information Memorandum, and the rationale for issuance of the BOD was summarized in your Decision Memorandum. As described further below, your decision to issue BOD 17-01 was based on three interrelated concerns that rested on expert judgments concerning national security: the broad access to files and elevated privileges of anti-virus software, including Kaspersky software; ties between Kaspersky officials and Russian government agencies; and requirements under Russian law that

[6] The BOD defines "Kaspersky-branded products" as all "information security products, solutions, and services supplied, directly or indirectly, by AO Kaspersky Lab or any of its predecessors, successors, parents, subsidiaries, or affiliates." The BOD explicitly does not apply, however, to two specific Kaspersky services: Kaspersky Threat Intelligence and Kaspersky Security Training.

[7] As November 12 was a Sunday, the deadline for submission was pushed to the next business day: Monday, November 13.

[8] Day 90 is December 12. However, DHS previously communicated to agencies that Day 90 is December 13. This arose because, as described above, Day 60 was November 12 (a Sunday), the agency submission due date was pushed to Monday, November 13, and 30 days from November 13 is December 13. As such, in practice, agencies may start removal, pursuant to the BOD, on December 13.

[9] 44 U.S.C. §§ 3552(b)(1), 3553(b).

allow Russian intelligence agencies to request or compel assistance from Kaspersky and to intercept communications transiting between Kaspersky operations in Russia and Kaspersky customers, including U.S. government customers. Because of these interrelated concerns, you determined that Kaspersky-branded products present a "known or reasonably suspected information security threat, vulnerability, or risk." In addition, you found that these risks exist regardless of whether Kaspersky-branded products have ever been exploited for malicious purposes. The BOD is a tool for protecting federal information and information systems from any "known or reasonably suspected information security threat, vulnerability, or risk," and the Department's authority to issue it does not depend on whether Kaspersky-branded products have been exploited by the Russian Government or Kaspersky to date.

DHS published the BOD in the *Federal Register* on September 19, 2017.

A. Administrative Process and Other Information Gathering

1. Kaspersky Submission

On the day the BOD was issued, you sent Kaspersky a letter enclosing the Decision Memorandum. The letter also explained an administrative process that DHS made available to Kaspersky and to any other entity that claimed its commercial interests were directly impacted by the BOD. This administrative process also was published in the *Federal Register*. The administrative process permitted Kaspersky and other entities to initiate a review of the BOD by submitting to DHS "a written response and any additional information or evidence supporting the response, to explain the adverse consequences, address the Department's concerns or mitigate those concerns."

At the request of counsel for Kaspersky, DHS also sent to Kaspersky's counsel on September 29, 2017 the full Information Memorandum and exhibits to ensure that Kaspersky had the complete unclassified rationale for issuance of the BOD. Kaspersky also stated publicly that it was "grateful for the opportunity to provide additional information" to DHS as part of the administrative process.[10]

The administrative process requires that I, or another official designated by you, "review the materials relevant to the issues raised by the [submitting] entity" and issue a recommendation to you regarding the matter. Your decision then needs to be communicated to the submitting entity by December 13, 2017. However, to complete the administrative process before agencies are required to start removal of Kaspersky software, I recommend that you respond to Kaspersky and issue your Final Decision on or before Monday, December 11.

DHS received a lengthy submission from Kaspersky on November 10, 2017, after granting Kaspersky a one week extension, at the request of Kaspersky's counsel, beyond the original November 3 deadline published in the *Federal Register*. As stated in footnote 1 above, the full Kaspersky Submission, including seven exhibits, is provided as Attachment D to the Action

[10] Exhibit 5 (Kaspersky Lab Response to Issuance of DHS Binding Operational Directive 17-01, Sept. 13, 2017, https://usa.kaspersky.com/about/press-releases/2017_kaspersky-lab-response-to-issuance-of-dhs-binding-operational-directive-17-01).

memorandum to which this memorandum is attached. DHS has not received a submission from any other entity.

On November 29, DHS met with two Kaspersky U.S. officials and their counsel, attorneys from Baker and McKenzie LLP. The meeting included a discussion of the Kaspersky Submission and related topics, including: Kaspersky's corporate structure; the alleged effects to the company's business that it attributes to U.S. government actions generally (not specific to the BOD); the NDAA provision discussed in Section II.B below; Kaspersky's intention not to target federal business and instead focus on enterprise and consumer customers; Kaspersky's view that any BOD should address software and other IT procurement risks generally, and not apply only to Kaspersky; and Kaspersky's mitigation proposals, discussed in Section III.A.2 below. Kaspersky did not present any new mitigation proposals beyond the limited proposals presented in the Kaspersky Submission.

2. Other Kaspersky Statements

Kaspersky, including Eugene Kaspersky, has made numerous statements publicly since the issuance of the BOD, including the following admissions and comments:

- Kaspersky's back-end servers, as well as a portion of its Kaspersky Security Network ("KSN") front-end servers, are located in Russia.[11]
- Kaspersky anti-virus software operates like other anti-virus software and thus has broad access to files and operates with the highest levels of system privileges.[12]
- In one instance, Kaspersky's software automatically pulled back classified Word files, contained in an archive file with other files that Kaspersky identified as malicious, from the alleged home computer of an NSA contractor.[13]

3. Information from Agencies

Since issuance of the BOD, all federal civilian executive branch agencies have reported to DHS on whether they identified Kaspersky-branded products on their federal information systems. Based on agency reports in response to the BOD and other communications between DHS and the agencies, DHS gained information about, among other matters, the types of Kaspersky products deployed on federal networks (enterprise vs. consumer, local vs. cloud-based); the types of Kaspersky services provided to federal customers; the types of devices that Kaspersky

---

[11] Exhibit 6 (Kaspersky Lab, *Principles for the processing of user data by Kaspersky Lab security solutions and technologies*, https://usa kaspersky.com/about/data-protection).

[12] Exhibit 7 (Kaspersky Lab, *Investigation Report for the September 2014 Equation malware detection incident in the US*, Secure List, 16 November 2017, https://securelist.com/investigation-report-for-the-september-2014-equation-malware-detection-incident-in-the-us/83210/) ("Kaspersky Lab security software, like all other similar solutions from our competitors, has privileged access to computer systems to be able to resist serious malware infections and return control of the infected system back to the user. This level of access allows our software to see any file on the systems that we protect.")

[13] *See* Exhibit 7 (Kaspersky Lab, *Investigation Report for the September 2014 Equation malware detection incident in the US*, 16 November 2017, https://securelist.com/investigation-report-for-the-september-2014-equation-malware-detection-incident-in-the-us/83210/).

products protect (endpoint vs. server); and the use of Kaspersky products by government contractors.

In total, fourteen agencies identified Kaspersky-branded products on their federal information systems. Some of those agencies removed the software in advance of the BOD's requirement to start removal on Day 90, unless directed otherwise by DHS based on new information. These agencies acted on their own initiative pursuant to standard agency risk management responsibilities under the Federal Information Security Modernization Act of 2014. DHS did not advise these agencies to start removal in advance of Day 90. As required by the Day 60 reporting requirement, the remaining agencies have submitted detailed plans of action for removal of Kaspersky-branded products starting on Day 90, unless directed otherwise by DHS.

4. Report on Relevant Provisions in Russian Law

As indicated above, DHS engaged a leading academic and consultant in Russian law, Professor Peter Maggs of the University of Illinois College of Law. Professor Maggs prepared a Report, attached as Exhibit 1, which confirms the key aspects of Russian law discussed in my Information Memorandum and provides additional support for DHS's Russian law-related concerns. In particular, Professor Maggs explains that, under Russian law, private entities, including Kaspersky, are obligated to assist the Russian Federal Security Service ("FSB") in executing the FSB's intelligence and other activities; that the FSB can second military personnel to Kaspersky with Eugene Kaspersky's consent; that Kaspersky is obligated to install equipment and software that permits the FSB to monitor transmissions between Kaspersky in Russia and its customers, including U.S. government customers, and Kaspersky has other obligations to provide information to the FSB; that Kaspersky is required to provide the keys or other information needed for the FSB to decrypt encrypted transmissions between Kaspersky and its customers; and that no court order is required for any of the above activities. Further details from the Maggs Report are provided in Section III.A.4 below.

B. NDAA Prohibition on Kaspersky Products and Services

In November 2017, Congress passed the National Defense Authorization Act for Fiscal Year 2018 (the "NDAA"). Section 1634(a) of the NDAA provides that "[n]o department, agency, organization, or other element of the Federal Government may use, whether directly or through work with or on behalf of another department, agency, organization, or element of the Federal Government, any hardware, software, or services developed or provided, in whole or in part," by Kaspersky or related entities.[14] Section 1634(b) provides that this prohibition takes effect on October 1, 2018.[15]

Unlike the statutory provision, BOD 17-01's direction to remove Kaspersky-branded products from federal information systems is effective on December 12, 2017, unless DHS directs otherwise. As stated above, the NDAA prohibition is not effective until October 2018. Thus,

[14] Exhibit 3 (Excerpt from National Defense Authorization Act for Fiscal Year 2018, § 1634(a), https://www.congress.gov/115/bills/hr2810/BILLS-115hr2810enr.pdf).
[15] Exhibit 3 (Excerpt from National Defense Authorization Act for Fiscal Year 2018, § 1634(b), https://www.congress.gov/115/bills/hr2810/BILLS-115hr2810enr.pdf).

until October 1, 2018, the BOD's requirement to start removal on Day 90, unless modified or rescinded by you, is the operative prohibition on agency use of Kaspersky products. At the same time, the NDAA provision is likely to cause agencies and other elements of the Federal Government, to the extent that they currently use Kaspersky hardware, software, or services, to take removal steps in advance of October 2018 to comply with the provision as of October 1, 2018.

III. ANALYSIS OF KASPERSKY SUBMISSION

Your decision to issue BOD 17-01 was based on three interrelated concerns: the broad access to files and elevated privileges of anti-virus software, including Kaspersky-branded products; ties between Kaspersky officials and Russian government agencies; and requirements under Russian law that allow Russian intelligence agencies to request or compel assistance from Kaspersky and to intercept communications transiting between Kaspersky operations in Russian and Kaspersky customers, including U.S. government customers. The combination of these factors creates various risks that the access and privileges provided by Kaspersky software installed on federal networks could be exploited by the Russian Government, alone or in collaboration with Kaspersky.

As detailed below, the Kaspersky Submission does not meaningfully address these concerns. Indeed, in certain statements, it confirms DHS's concerns, as do the Maggs Report and the NCCIC Supplemental Assessment. The Kaspersky Submission also does not present any new or comprehensive mitigation proposal to address these risks.

The analysis below is divided into two parts. First, I address aspects of the Kaspersky Submission that respond to the DHS concerns communicated to the company. I then address additional information and arguments presented by Kaspersky.[16]

[16] The Kaspersky Submission also provides information on certain topics that I have not addressed below because the information does not directly relate to the information security risks presented by Kaspersky-branded products. For example, Kaspersky includes a description of its corporate structure that was not previously available to DHS. DHS now understands that AO Kaspersky Lab is wholly owned by Kaspersky Labs Limited ("KLL"), a United Kingdom company, through OOO Kaspersky Group, a Russian corporation, and Eugene Kaspersky personally owns over 80 percent of KLL's stock. *See* Kaspersky Submission at 7. The fact that the ultimate parent entity is a UK company does not affect the applicability of the Russian law provisions discussed below, which apply to legal entities, operations, and individuals in Russia, including Kaspersky headquarter operations in Moscow. Kaspersky also provides information on its sales to U.S. government customers and negative financial effects that Kaspersky attributes to the BOD. *See* Kaspersky Submission at 2, 7-8, 33. Furthermore, Kaspersky notes that the list of Kaspersky products in the Information Memorandum is "inconsistent" with the final list of Kaspersky products in the BOD. *See* Kaspersky Submission at 9-10. That is true, but also intentional. Between the issuance of the Information Memorandum on September 1 and your issuance of the BOD on September 13, DHS decided to group products with similar names using a general term, rather than listing numerous specific products individually. For example, DHS grouped distinct products under the general term "Kaspersky Endpoint Security" and distinct cybersecurity services under the general term "Kaspersky Cybersecurity Services." This did not affect the scope of the BOD, since the BOD applies to *all* products, solutions, and services supplied, directly or indirectly, by Kaspersky, with the exception of two specific services. Kaspersky also states that DHS's inclusion of "Kaspersky Cloud Security (Enterprise)" indicates a lack of understanding about Kaspersky's product portfolio and the functionality of Kaspersky products. Kaspersky Submission at 9. On the contrary, DHS understands that Kaspersky Cloud Security is not a discrete product offering, and instead refers to a set of cloud security capabilities marketed to Enterprise customers, as described on this Kaspersky webpage: https://www kaspersky.co.in/enterprise-

A. Kaspersky Responses to Specific Concerns in the Information Memorandum

1. NCCIC and BRG Assessments

i. Overview

Exhibit 1 to the Information Memorandum was an Information Security Risk Assessment prepared by the NCCIC (the "NCCIC Assessment"). The NCCIC Assessment analyzed the information security risks of anti-virus software generally and Kaspersky-branded products specifically. Among other information security risks, the NCCIC Assessment explained that anti-virus software, including Kaspersky-branded products, needs to operate with broad access to files and high-level system privileges in order to identify and remediate system threats. This functionality could be exploited by a malicious cyber actor to conduct a wide range of cyber attacks against systems and networks running Kaspersky anti-virus software. Like nearly all software, Kaspersky anti-virus also receives software updates that could include malware, or the software's signature updates could withheld to allow a specific attack.

Kaspersky discounts the NCCIC Assessment, asserting that it consists of "general" and "conclusory" allegations and is not based on independent testing and evaluation of Kaspersky products. To address this alleged deficiency, Kaspersky's outside counsel at Baker & McKenzie LLP retained Berkeley Research Group, LLC ("BRG"), a self-described "leading global strategic advisory and expert services firm."[17] BRG's assessment, titled "Information Security Risks of Anti-Virus Software" (the "BRG Assessment"), is provided as Exhibit B in the Kaspersky Submission.

The majority of the BRG Assessment argues that the risks that DHS has identified with respect to Kaspersky anti-virus software also exist with respect to other anti-virus software supplied by other vendors to federal agencies. These arguments are addressed in Section III.B.2 below.

The remainder of the BRG Assessment, sub-titled "Preliminary Review of Kaspersky Lab Software," explains BRG's initial testing of various Kaspersky products across three objectives (described below).[18] The Kaspersky Submission does not discuss BRG's preliminary review. NCCIC reviewed this portion of the BRG Assessment and prepared a supplementary analysis (the "NCCIC Supplemental Assessment"), which is attached as Exhibit 2.

ii. High-Level Comments

Kaspersky and BRG fault DHS for not conducting a technical assessment of Kaspersky's products.[19] But DHS's determination that Kaspersky-branded products present an information

security/cloud-security. Finally, Kaspersky correctly notes that Kaspersky Threat Intelligence and Kaspersky Security Training services are explicitly excluded from the scope of the BOD. Thus, while the BOD applies to most Kaspersky Cybersecurity Services, the BOD does not apply to these two services, and DHS has not "simultaneously prohibited procurement" of these services. *See* Kaspersky Submission at 10.

[17] Kaspersky Submission at 11; BRG Assessment at 36.

[18] *See* BRG Assessment at 23-30.

[19] *See* BRG Assessment at 6; Kaspersky Submission at 9.

security risk to federal information and information systems was not based on unique technical aspects of Kaspersky-branded products, but rather the broad access and privileges that anti-virus products have by their nature, combined with the location of Kaspersky's servers and other operations in Russia, ties between Kaspersky officials and Russian officials, and the authorities provided to Russian government agencies under Russian law.

In addition, far from refuting the NCCIC Assessment, the BRG Assessment confirms some of its key conclusions. As described further in the NCCIC Supplemental Assessment, BRG explains, consistent with the NCCIC Assessment, that anti-virus software operates with "broad access to the computer's hardware and operating system" and that the software "runs with the same privileges as the user, as well as one or more underlying, highly-privileged software components, such as kernel-mode drivers or SYSTEM-level processes."[20]

iii. BRG's Technical Analysis and the NCCIC Supplemental Assessment

BRG evaluated specific Kaspersky products according to the following objectives:

(1) To evaluate whether it is feasible for an intelligence agency to passively monitor and decrypt traffic between users of Kaspersky-branded products and the Kaspersky Security Network ("KSN"), a cloud-based network that receives and analyzes information about possible threats from installed Kaspersky software;
(2) To determine whether turning KSN off — or using the Kaspersky Private Security Network ("KPSN") — can reliably prevent potentially sensitive data from being transmitted inadvertently to Kaspersky; and
(3) To evaluate whether a malicious actor leveraging KSN can conduct targeted searches of Kaspersky users for specific information.

As explained in the NCCIC Supplemental Assessment, the BRG analysis not only is largely unresponsive to DHS's security concerns, but also supports DHS's concerns in certain areas. For example, on objective (1), BRG analyzed only to the security of the connection between the anti-virus software and the KSN; BRG did not address the security of communications within the KSN or between KSN and Kaspersky's non-KSN IT infrastructure, such as Kaspersky offices and datacenters.[21] BRG also evaluated the potential for "passive" interception of communications by intelligence agencies, but DHS is concerned about "active" operations involving access by Russian intelligence to Kaspersky offices and servers in Russia, as discussed in Section III.A.4 below and Part III.E of the Information Memorandum.

On objective (2), BRG determined that user data was transmitted to Kaspersky even when a user turned KSN off, and did not address the risks of using the KPSN, which is the on-premise version of the KSN.. I address objective (2) further in Section III.A.2 below.

On objective (3), BRG determined that Kaspersky's anti-virus software can be used to retrieve and upload files and other data from user's computers without the user necessarily being

[20] BRG Assessment at 11.
[21] *See* BRG Assessment at 24 n.71.

notified.[22] Moreover, BRG concedes that it has not reviewed "Kaspersky's operational processes related to any controls surrounding the development, testing, deployment, and auditability of records [the basis for Kaspersky pulling back malware and other files] given their capabilities and breadth of system access."[23] Thus, BRG presented no evidence undermining DHS's concerns about Kaspersky software being used to pull non-malicious files from users computers.

iv. Kaspersky Services

As you know, the BOD applies not only to software but also to Kaspersky services, with two specific exceptions. The NCCIC Assessment states that the Kaspersky services subject to the BOD, including threat hunting, incident response, and security assessment services, present various information security risks, with the specific risks dependent on the specifics of the service provided. In general, however, NCCIC determined 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."[24]

Kaspersky states that this portion of the NCCIC Assessment is conclusory,[25] but neither Kaspersky nor the BRG Assessment provide any evidence or explanation why the Kaspersky services covered by the BOD, including threat hunting, incident response, and security assessment services, do not present the information security risks identified by the NCCIC.

v. No Need for Evidence of Wrongdoing

Without disputing that its software operates with elevated access and privileges, Kaspersky argues that DHS has not presented "any evidence of wrongdoing" by Kaspersky or any evidence that Kaspersky products have been "subject to (or leveraged for) any of the information security risks identified by DHS.[26]

This argument misunderstands the purpose of the BOD and the standard for issuing it. Congress granted you the authority to issue BODs based on any known or reasonably suspected information security threat, vulnerability, or risk. For the reasons stated in the Information Memorandum and its attached NCCIC Assessment, Kaspersky-branded products meet that standard. And, as you stated in your Decision Memorandum, "[t]hese risks exist regardless of whether Kaspersky-branded products already have been used by Kaspersky or the Russian Government for malicious purposes."

2. Proposed Mitigations: Kaspersky Security Network, Kaspersky Private Security Network, and Use of Multiple Anti-Virus Products

[22] *See* BRG Assessment at 29-30; NCCIC Supplemental Assessment at 10.
[23] BRG Assessment at 30.
[24] Exhibit 4.A (NCCIC Assessment at 6-7).
[25] *See* Kaspersky Submission at 10.
[26] Kaspersky Submission at 2.

Kaspersky argues that DHS has not accounted for reasonable measures that may mitigate the risks presented by Kaspersky products and services.[27] The Kaspersky Submission, however, contains no clear or comprehensive mitigation proposal. Rather, in two limited sections of the Kaspersky Submission and objective (2) in the BRG "Preliminary Review," Kaspersky appears to suggest that federal agencies: (1) either choose not to participate in the Kaspersky Security Network ("KSN") or deploy the local Kaspersky Private Security Network ("KPSN"); and (2) install one or more additional anti-virus solutions, in addition to Kaspersky anti-virus software, to address the risk that Kaspersky's software may not include necessary signature updates. Kaspersky did not offer any other mitigation proposal in its in-person meeting with DHS on November 29, 2017.

First, these options address, at best, only a limited set of the information security risks identified by DHS. For example, none of these options address the risk that the Russian government, without the company's knowledge or cooperation, or Kaspersky, in collaboration with Russia, can exploit the high-level privileges of the software to install malware on government computers.[28] As discussed in Section III.B of the Information Memorandum and the NCCIC Assessment, such malware could jeopardize the integrity or availability of federal information or information systems, and potentially be used to exfiltrate files outside of any customer connection with the KSN.

To the extent that these options address risks identified by DHS, they also are insufficient or impractical. For example, DHS understands that the KSN allows Kaspersky users to offload certain detection processing to external servers that receive data on new threats from other Kaspersky KSN participants around the world.[29] Government customers that decline this participation may reduce the risk of sensitive files and other data being uploaded to the KSN, but these customers also would lose at least some of the threat detection benefits of participating in the KSN.

Further, according to the End User License Agreements ("EULAs") for Kaspersky products, including for Kaspersky Anti-Virus 2013 and Kaspersky Anti-Virus 2018, Kaspersky customers do transmit data to Kaspersky's network even if they decline participation in the KSN. Based on the EULA for Kaspersky Anti-Virus 2013, which Kaspersky references in this section of its submission, the end-user agrees to provide to Kaspersky various information such as the following:

- To increase operational protection: Certain data ("checksums") representing files processed, information to determine the reputation of URLs, information about the types of identified threats, digital certificates used and "information necessary to verify their authenticity."

[27] *See* Kaspersky Submission at 3.
[28] *See* Section III.A.4 below.
[29] *See, e.g.,* Exhibit 6 (Kaspersky Lab, *Principles for the processing of user data by Kaspersky Lab security solutions and technologies*, https://usa kaspersky.com/about/data-protection).

- If the computer is equipped with Trusted Platform Module ("TPM"): The TPM report about the computer operating system boot process and "the information necessary to verify the authenticity of the report."[30]

The EULA for the more recent Kaspersky Anti-Virus 2018 requires users, including non-KSN-participants, to automatically provide a broader set of information, including the following:

- Information about installed programs;
- Information on detected threats and infections;
- Checksums of processed objects;
- Technical information about the computer and devices connected to it; and
- Information about online activity of the device.[31]

BRG similarly determined that Kaspersky "consumer-oriented products," which may be used by federal agencies, "communicated with KSN to a limited degree *despite declining to agree to the KSN Statement during product installation and also disabling KSN within the application's user interface*" (emphasis added).[32] BRG does not provide a full description of the data uploaded to KSN, but BRG states that it "infers" that "statistics" about detection of a malware file were uploaded to Kaspersky, and the file itself was "likely uploaded to Kaspersky when KSN was enabled."[33]

Kaspersky also states that "[a]ll data transferred via the KSN is aggregated and anonymous; Kaspersky Lab does not attribute data to identified individuals" (emphasis added).[34] This statement appears to be imprecise and overbroad based on prior Kaspersky statements. First, by contrast with the EULA for Kaspersky Anti-Virus 2013, which provides that "[t]he Software does not process any personally identifiable data and does not combine the processed data with any personal information[,]"[35] the EULA for Kaspersky Anti-Virus 2018 includes no such representation.[36] This omission appears to be a telling one. Indeed, in the Information Memorandum, I quoted the following from the KSN Statement: "Kaspersky Lab uses the information received only in an anonymized form as part of aggregated statistics. These aggregated statistics are generated automatically from the original information received and do not contain personal information or any other confidential information. Initial information received is destroyed upon accumulation (once a year). General statistics are kept indefinitely."[37] I noted that, if a customer participates in the KSN, "it appears that Kaspersky

---

[30] *See* Exhibit 8 (End-User License Agreement for Kaspersky Anti-Virus 2013, 19 March 2013, § 5, https://support kaspersky.com/8752).
[31] *See* Exhibit 9 (End-User License Agreement for Kaspersky Anti-Virus 2018, 21 August 2017, § 6, https://support kaspersky.com/13596).
[32] BRG Assessment at 28.
[33] BRG Assessment at 28.
[34] Kaspersky Submission at 14.
[35] Exhibit 8 (End-User License Agreement for Kaspersky Anti-Virus 2013, 19 March 2013, § 5.4, https://support kaspersky.com/8752)
[36] *See generally* Exhibit 9 (End-User License Agreement for Kaspersky Anti-Virus 2018, 21 August 2017, https://support kaspersky.com/13596).
[37] Exhibit 4 (Information Memorandum at 19) (quoting the KSN Statement for Kaspersky Endpoint Security 10 for Windows, Section B).

obtains 'original information' and retains that information for one year, apart from any anonymized, aggregated 'use' of that data."[38] I also referred to the NCCIC Assessment, which explained that this information could contain a range of data that identifies customers, such as user account names, computer names, and file paths, even if not combined with Kaspersky subscription information or contact lists.[39] Neither Kaspersky nor BRG provides any information or arguments to rebut these concerns.

DHS, including the NCCIC, also examined the information that Kaspersky and BRG provided about the KPSN. Specifically, as described in the BRG Assessment and the NCCIC Supplemental Assessment, the KPSN can be deployed in three possible configurations. BRG tested KPSN in its "Standard" configuration — which allows outbound connections between on-premise KPSN servers and Kaspersky servers directly and, in response to a malware detection test, BRG observed traffic between its enterprise Kaspersky software and the KPSN servers, but not any traffic between the KPSN server and the KSN or any other Kaspersky server.

As stated above, however, the KPSN deployment option still receives software updates from Kaspersky, which could include malware or not include all updates needed to identify known cybersecurity threats. Such malware, for example, could compromise the integrity or availability of data or services on a local agency network, even if no data is transmitted back to Kaspersky. Such risks exist even if agencies deployed KPSN in its "Unidirectional Gateway" configuration, in which a gateway in the organization's "demilitarized zone" allows only inbound traffic to on-premise KPSN servers.[40] Kaspersky's characterization of these risks as "purely theoretical, speculative, and conclusory"[41] is not evidence rebutting the risks, particularly in light of the discussion in the BRG Assessment about malware and vulnerabilities in anti-virus products, which presumably existed in the software in its original installation or were introduced into the software, and thus on to the user's computer, through a software update or upgrade.[42]

Finally, Kaspersky and the BRG Assessment argue, citing NIST Special Publication 800-83, Revision 1, that the risk of Kaspersky intentionally withholding signatures to allow specific attacks can be mitigated by using "multiple layers of anti-virus protection at the host and network level."[43] The determination to issue BOD 17-01 was based on a combination of concerns, not on the withholding of signatures in isolation. However, for the sake of argument, the NIST publication that Kaspersky cites also states that "running multiple antivirus products on a single host simultaneously is likely to cause conflicts between the products" and thus, "if multiple products are used concurrently, they should be installed on separate hosts" (*e.g.*, one anti-virus product on perimeter email servers and a different product on internal email servers).[44] NIST also notes that this "would necessitate increased administration and training, as well as

[38] Exhibit 4 (Information Memorandum at 19).
[39] Exhibit 4 (Information Memorandum at 19).
[40] BRG Assessment at 28-29.
[41] Kaspersky Submission at 15.
[42] *See* BRG Assessment at 12-16.
[43] Kaspersky Submission at 15; BRG Assessment at 35.
[44] Exhibit 10 (Excerpt from NIST Special Publication 800-83, Rev. 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, July 2013, at 11, http://nvlpubs nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf).

additional hardware and software costs."[45] DHS cannot reasonably expect that federal agencies buy and deploy additional anti-virus software, and bear the attendant costs and technical challenges, in connection with a mitigation measure that does nothing to address the various access and privilege risks raised by Kaspersky software.

3. Kaspersky Ties to the Russian Government

In the Information Memorandum, I described certain ties, past and present, between Kaspersky officials and Russian government agencies.[46] Kaspersky concedes key aspects of this account, such as Eugene Kaspersky's former studies at an institute overseen by the KGB and other state institutions and his service as a software engineer at a Ministry of Defense institute.[47] It also admits that its officials might have "acquaintances, friends, and professional relationships within the [Russian] government," although Kaspersky states that, "in itself," does not mean that these connections were or are "inappropriate" or "improper."[48] Furthermore, Kaspersky does not deny various connections to Russian intelligence described in the Information Memorandum, including that Eugene Kaspersky has saunas with a group that usually includes Russian intelligence officials; that Kaspersky's Chief Legal Officer Igor Chekunov manages a team of specialists who provide technical support to the FSB and other Russian agencies; that the team can gather identifying information from individual computers; and that this technology has been used to aid the FSB in investigations.[49]

In the Information Memorandum, I also briefly addressed a *Bloomberg* article from July 2017 that reported, based on internal Kaspersky emails, that "Eugene Kaspersky was overseeing the development of a secret anti-hacking software project for the FSB," and "[t]hat project became the basis of Kaspersky's anti-denial-of-service security technology."[50] The Kaspersky Submission states that 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."[51] Moreover, Kaspersky states that "[s]uch an engagement if it were to be true, would be anything but inappropriate given Kaspersky Lab's technology and expertise." Kaspersky raises a valid point that the alleged relationship with respect to anti-DDoS technology, if true, relates to a defensive use of software, and thus is not the type of relationship between the FSB and Kaspersky that is of most concern to DHS. Nonetheless, this project, if true, is evidence that Kaspersky has developed software for or in collaboration with the FSB. Such an established relationship and connections between Kaspersky and the FSB could facilitate future cooperation for other purposes and therefore is an area of serious concern to DHS. Kaspersky further states that "the Russian Government's anti-cybercrime unit told the company that it considered DDoS attacks an emerging and serious threat" and that the FSB "has never been[] a Kaspersky Lab

---

[45] Exhibit 10 (Excerpt from NIST Special Publication 800-83, Rev. 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, July 2013, at 11, http://nvlpubs nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf).
[46] *See* Exhibit 4 (Information Memorandum at 10-11).
[47] Kaspersky Submission at 17.
[48] Kaspersky Submission at 16-17.
[49] *See* Exhibit 4 (Information Memorandum at 10-11).
[50] Exhibit 4 (Information Memorandum at 10).
[51] Kaspersky Submission at 18.

DDoS Protection client."[52] It is unclear whether these statements are intended to suggest, contrary to the *Bloomberg* report, that Kaspersky has *never* developed software for or in collaboration with the FSB. In any event, as further described below, Kaspersky is required to collaborate with Russian government entities under Russian law.

4. Risks Arising under Russian Law

DHS has retained Professor Peter Maggs, a leading Russian law scholar, to advise the Department and to prepare a report (the "Maggs Report") on various aspects of Russian law, including on the ability of Russian government agencies, including the FSB, to compel or request assistance from Kaspersky. Professor Maggs is a Professor of Law Emeritus at the University of Illinois College of Law; he speaks, reads, and writes Russian fluently; and he is the author, co-author, co-editor, translator, or co-translator of a dozen books and numerous articles on Soviet and Russian law, including a translation of the Russian Civil Code.[53] The Maggs Report is provided as Exhibit 1.

The Maggs Report was prepared based on extensive research and analysis by Professor Maggs, including reviewing, in Russian, Russian laws, amendments to those laws, and other legal authorities, among other sources. He then translated key provisions into English for inclusion in the Maggs Report.

Professor Maggs makes a number of significant conclusions. Specifically, Professor Maggs concludes that:

(a) Russian law requires FSB bodies to carry out their activities in collaboration with various entities in Russia, including private enterprises, and thus including Kaspersky.

(b) Private enterprises, including Kaspersky, are under a legal obligation to assist FSB bodies in the execution of the duties assigned to FSB bodies, including counterintelligence and intelligence activity.

(c) Russian law permits FSB service personnel to be seconded to private enterprises, including Kaspersky, with the consent of the head of the enterprise and with the FSB personnel remaining in FSB military service status during the secondment.

(d) Kaspersky qualifies as an "organizer of the dissemination of information on the Internet" and, as such, is required (1) to store in Russia and provide to authorized state bodies, including the FSB, metadata currently and content as of July 1, 2018; and, based on this or other laws, (2) to install equipment and software that enables the FSB and potentially other state authorities to monitor all data transmissions between Kaspersky's computers in Russia and Kaspersky customers, including U.S. government customers.

[52] Kaspersky Submission at 18.
[53] Exhibit 1 (Maggs Report at ¶ 9).

(e) No court order is required for FSB operational-investigative activities undertaken in the performance of FSB duties, including operational-investigative activities involving the obtaining of information stored on and communications with United States government computers, and Kaspersky is obligated to assist the FSB with such operational-investigative activities.

(f) Kaspersky is required to provide the FSB and other Federal executive bodies in the field of security with the keys or other information needed to decrypt Kaspersky's encrypted data transmissions.

Each of these conclusions, independently and collectively, present significant risks of action by the Russian Government, alone or in collaboration with Kaspersky, that create a risk to federal information and information systems. These conclusions also are consistent with DHS's analysis of Russian law before retaining Maggs and during the engagement.

Key aspects of the above analysis were presented in the Information Memorandum, such as the FSB's authority to compel or request assistance from companies in Russia.[54] I also described the FSB's ability to intercept data transmissions made over Russian telecom and Internet Service Provider networks.[55]

The Kaspersky Submission concedes various aspects of these conclusions. For example, Kaspersky concedes that "[a]ll 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, including very broadly defined duties such as "informing state authorities of security threats"; "detecting and preventing foreign intelligence activities"; "obtaining intelligence information in the interests of state security" and "increasing the state's economic, scientific, technical and defense capabilities"; and "providing for various types of security of the Russian Federation."[56] Kaspersky states starkly: "If a company operating in Russia receives a request from the FSB for information, it must comply with such request."[57]

Kaspersky cautions that "the FSB's powers in this regard are not unlimited, and FSB requests are subject to challenge in court."[58] However, the FSB does not need a court order to obtain information stored on and communications with United States government computers. Instead, court approval is only needed for the interception of Russian Constitutionally-protected personal communications, and such protections generally would not apply to transmissions sent to or received from anti-virus software on U.S. government computers. Furthermore, on the ability to challenge FSB requests in court, Maggs' research did not reveal a single case brought against the FSB by a party seeking to avoid cooperation with the FSB.[59]

Kaspersky attempts to justify these authorities by equating them with United States laws. Specifically, Kaspersky states that "[s]imilar laws exist in the U.S. to compel companies to hand

[54] *See* Exhibit 4 (Information Memorandum at 12-13).
[55] *See* Exhibit 4 (Information Memorandum at 13).
[56] Kaspersky Submission at 19.
[57] Kaspersky Submission at 19.
[58] Kaspersky Submission at 19.
[59] Exhibit 1 (Maggs Report at ¶ 38).

over customer data and any other information," and that the U.S. Department of Justice has recently expressed a desire to mandate that technology companies provide encryption keys to law enforcement.[60] These general comparisons to the U.S. are irrelevant; DHS is only concerned, with respect to BOD 17-01, about information security risks arising from Kaspersky-branded products.

Kaspersky also argues that it is not subject to Russian requirements that telecommunications companies and Internet Service Providers install equipment that permits FSB surveillance of communications and other data transmissions over their networks because the company does not "provide communication services."[61] But Kaspersky arguably is required to install hardware and/or software in its network that permits FSB monitoring of data transmissions between Kaspersky in Russia and Kaspersky customers, including U.S. government customers, under one or more laws.[62] In addition, Kaspersky does not deny that its data transmissions with customers, including U.S. government customers, occur over Russian telecom and ISP networks that are subject to interception by the FSB. And, as explained above, Professor Maggs identified a legal provision requiring Kaspersky to provide the decryption keys or other information needed to decrypt its encrypted communications over these networks.[63]

Further, Kaspersky incorrectly states that any such interception by the FSB either requires prior court approval or, in certain emergency situations, notification to a court within 24 hours and court approval within 48 hours. However, as indicated above, court approval is only needed for interception of Russian Constitutionally-protected personal communications, and such protections would not apply to transmissions sent to or received from anti-virus software on U.S. government computers.[64]

Finally, in a separate section of the Kaspersky Submission, Kaspersky states that all U.S. operations and sales are "driven through" Kaspersky Lab, Inc., a Massachusetts corporation that is headquartered in Woburn, Massachusetts and is a direct wholly-owned subsidiary of Kaspersky Labs Limited, a UK company described in footnote 11 above. Kaspersky admits, however, that its headquarters, back-end servers, and a portion of its front-end KSN servers are located in Russia, and therefore Kaspersky customer data is stored in Russia or accessible from Russia.[65] As such, Kaspersky's statement that there are "no Russian companies in the ownership structure of Kaspersky Lab, Inc."[66] is not responsive to the Russia-related risks identified by DHS.

5. Kaspersky Licenses and Certificates

On page 20 of its Submission, Kaspersky describes the role of a subdivision of the FSB in issuing licenses to companies involved in encryption-related activities. DHS does not dispute

[60] Kaspersky Submission at 19.
[6161] *See* Kaspersky Submission at 21.
[62] *See* Exhibit 1 (Maggs Report at ¶¶ 42-52).
[63] *See* Exhibit 1 (Maggs Report at ¶¶ 31, 55).
[64] *See* Exhibit 1 (Maggs Report at ¶¶ 29-30, 55).
[65] Exhibit 6 (Kaspersky Lab, *Principles for the processing of user data by Kaspersky Lab security solutions and technologies*, https://usa kaspersky.com/about/data-protection).
[66] Kaspersky Submission at 7.

that one or more components of the FSB are involved in such licensing, or that the U.S. Department of the Treasury, Office of Foreign Assets Control issued a general license authorizing certain otherwise prohibited transactions with the FSB to obtain such licenses.[67] Rather, in my Information Memorandum, I expressed concern that the Russian government could impose conditions as part of the issuance of such licenses or certificates, such as a condition requiring that Kaspersky or Russian telecommunications providers provide keys to decrypt encrypted data transmissions or otherwise provide access to customer data.[68] The Kaspersky Submission does not deny or otherwise address these concerns.

Nor does Kaspersky offer a meaningful response to the specific concerns raised in the Information Memorandum about certificates issued in 2007 and 2011 to Kaspersky Lab and Military Unit ("MU") 43753. Kaspersky states, without explanation, that MU 43753 "is the FSB department responsible for the protection of information." Kaspersky then states that the FSB issued the 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."[69] Kaspersky's use of "presumably" indicates that Kaspersky does not know why the certificates were also issued to MU 43753, and thus does not have confidence in its explanation. Professor Maggs also states that Kaspersky likely has documentation in its files that would explain the relationship, but such materials are not discussed in Kaspersky's submission.[70]

6. Statements and Actions by Other Federal and State Officials

The Information Memorandum describes statements and actions by U.S. Intelligence Community agency heads; the Chairman of the House Science Committee; the General Services Administration ("GSA"); and the California Department of General Services, all of whom expressed concern with the information security risks presented by Kaspersky products.[71]

Kaspersky argues that this portion of the Information Memorandum is "irrelevant" and the reasoning "circular," and it criticizes each reference individually.[72] I do not agree with Kaspersky's characterizations and critiques. Contrary to Kaspersky's assertions, DHS has extensive evidence to support the BOD independent of these statements, which were offered simply to show that other officials reached the same conclusion as DHS, before issuance of the BOD, that Kaspersky products present information security risks.

By way of example regarding Kaspersky's specific critiques, Kaspersky argues that Chairman Lamar Smith issued letters to agency heads about Kaspersky because the Committee was conducting oversight related to the NIST Framework.[73] While I agree that Chairman Smith focuses on NIST pursuant to the House Science Committee's jurisdiction over NIST, these comments ignore the substance of Chairman Smith's letter, which clearly express concern that

---

[67] *See* Kaspersky Submission at 20.
[68] *See* Exhibit 4 (Information Memorandum at 13).
[69] Kaspersky Submission at 21.
[70] *See* Exhibit 1 (Maggs Report at ¶ 41).
[71] *See* Exhibit 4 (Information Memorandum at 14-15).
[72] Kaspersky Submission at 22-26.
[73] *See* Kaspersky Submission at 23-24.

Kaspersky products can be used as a tool for nefarious actions against the United States.[74] For example, the letter states: "The Committee is concerned that Kaspersky Lab is susceptible to manipulation by the Russian government, and that its products could be used as a tool for espionage, sabotage, or other nefarious activities against the United States."[75]

Kaspersky also discusses testimony by the GSA Chief Information Officer, who stated that GSA directed three resellers to remove Kaspersky products from GSA schedule contracts because the resellers "did not gain approval to do so via the required contract modification process,"[76] rather than because of any reasons related to Kaspersky.[77] However, GSA has stated publicly that its basis for removing Kaspersky products from two GSA schedules was the information security risks presented by the products, not because of a technical, contractual failure by the these suppliers. Specifically, GSA stated in response to press inquiries about GSA's reasons for the removals: "GSA's priorities are to ensure the integrity and security of U.S. government systems and networks and evaluate products and services available on our contracts using supply chain risk management processes."[78]

B. Additional Information and Arguments in Kaspersky Submission

1. Kaspersky's Positive Reputation and Activities

Kaspersky argues that it is a "market-leading" company; that it is "consistently recognized by its peers, the industry, and consumer groups for developing best-in-class cyber-protection tools," including receiving top product rankings; that it "leads the world in cyberthreat assessment and analysis"; that its researchers and analysts in its Global Research & Analysis Team ("GReAT") have identified numerous cyberthreats originating in Russia and/or in the Russian language; that it collaborates with well-known IT security vendors in conducting joint cyberthreat investigations; and that it collaborates with law enforcement agencies and elements of the U.S. government in fighting cybercrime and sharing threat information.[79] Kaspersky states that "working inappropriately with the Russian Government would clearly be detrimental to the Company's bottom line," and therefore, "Kaspersky has a powerful economic incentive to never take any action that would endanger the trusted relationship and integrity that serve as the foundation of its business."[80]

---

[74] *See* Exhibit 4 (Information Memorandum at 15).
[75] Exhibit 11 (Letter from Chairman Smith to The Honorable Sonny Perdue, 27 July 2017, https://science.house.gov/sites/republicans.science house.gov/files/documents/072717%20Smith-Agencies%20-%20Kaspersky.pdf).
[76] Exhibit 12 (Statement of David Shive, Hearing Before the House Committee on Science, Space, and Technology Subcommittee on Oversight, *Bolstering the Government's Cybersecurity: Assessing the Risk of Kaspersky Lab Products to the Federal Government*, 25 October 2017, https://science.house.gov/sites/republicans.science house.gov/files/documents/HHRG-115-SY21-WState-DShive-20171025.pdf).
[77] *See* Kaspersky Submission at 25 and n. 112.
[78] Exhibit 13 (Eric Geller, *Trump Administration Restricts Popular Russian Security Software*, Politico, 11 July 2017, https://www.politico.com/story/2017/07/11/trump-russian-security-software-240423).
[79] *See* Kaspersky Submission at 1, 3-7; BRG Assessment at 30-33.
[80] *See* Kaspersky Submission at 7, 16.

DHS is aware that Kaspersky products have received top ratings for malware detection (among other performance factors) and that the company has received positive comments for its' research and analysis. However, these product ratings, by third-party testing organizations, test suitability for enterprise or consumer users generally; they were not conducted by government testing organizations or conducted for purpose of rating suitability for federal networks. More importantly, high malware detection ratings do not mean that Kaspersky products could not also be leveraged for malicious activities by Russian cyber actors. Indeed, on the company's reputation, Eugene Kaspersky admits in a blog post: "[W]e know awards and accolades don't address these recent allegations."[81] Finally, I am not persuaded that DHS should ignore the information security risks presented by Kaspersky-branded products based on the company's statement that it would not be rational to allow its products to be exploited for malicious purposes. As explained in Section III.A.4 above, under Russian law, Kaspersky does not have a choice on whether to assist the FSB and the FSB could exploit the access provided by Kaspersky products without Kaspersky's knowledge.

2. Comparison to Other Anti-Virus Products Sold to the U.S. Government

Kaspersky and BRG devote a substantial portion of their submissions to the argument that the federal government purchases anti-virus software from a range of suppliers, and there is no basis for the BOD to apply only to Kaspersky anti-virus software.

To support this argument, BRG identified other anti-virus software suppliers to the federal government using procurement information in a USASpending.gov database. Of approximately 20 different suppliers over the past 10 years, BRG selected six suppliers — Avast , AVG, ESET, McAfee, Symantec, and Trend Micro — in addition to Kaspersky, based on a number of factors, including estimated volume of purchasing contracts in either US dollars or number of licenses; comparability of software features to those of Kaspersky-branded products; and supplier affiliations with foreign countries or governments.[82] BRG then selected specific products developed by each of these companies, although BRG acknowledges that it does not know if these are the specific product versions in use at U.S. government agencies because of limitations in the public procurement data.[83]

Kaspersky argues that these software developers are "similarly situated" to Kaspersky — based on foreign affiliations of the companies, publicly-reported vulnerabilities in the software, and sensitive data collection by the software — but not subject to the BOD.[84]

For the reasons discussed below, none of these anti-virus developers or their products present the same information security risks that DHS has identified with respect to Kaspersky-branded products. In addition, this BOD is focused on the information security risks presented by Kaspersky-branded products, and DHS has no obligation to apply the BOD to all anti-virus products that might present some information security risk. Nonetheless, DHS will continue to

[81] Exhibit 14 (Eugene Kaspersky, *Proud to keep on protecting – no matter of false allegations in U.S. media*, Kaspersky Lab Blog, 19 October 2017, https://www kaspersky.com/blog/whats-going-on/19860/).
[82] *See* BRG Assessment at 9-10.
[83] *See* BRG Assessment at 11.
[84] *See, e.g.*, Kaspersky Submission at 2.

assess the risks presented to federal information and information systems, including by information technology products, and will take action where appropriate.

i. Foreign Affiliations of the Other Anti-Virus Suppliers

BRG highlights the following "foreign affiliations" of these software developers:[85]

- Headquarters Outside the U.S.: Avast (headquartered in the Czech Republic); ESET (headquartered in Slovakia); Trend Micro (headquartered in Taiwan until its relocation to Japan in 1998).
- Offices in Russia: Symantec, McAfee, Avast, and Kaspersky.
- Offices in China: Symantec,[86] McAfee, and Trend Micro.
- Servers Outside the U.S.: Avast (19 countries, including China and Russia).
- Product Communicates Directly with Servers Outside the U.S.: Avast (product communicates with server in the Czech Republic); ESET (product communicates with server in Slovakia).
- Product Relies on Third-Party Content Distribution Networks or Hosting Providers to Distribute the Software, Updates, Malware Signature Updates, or other Functionality: Trend Micro and Symantec (use Akamai); McAfee (uses Amazon Web Services).

These other anti-virus suppliers are not "similarly situated" to Kaspersky. Kaspersky is headquartered in Moscow, Russia and its back-end servers are located in Russia.[87] This presents a substantially greater risk of exploitation than other anti-virus software developed by companies headquartered in the Czech Republic, Slovakia, or Japan (none of which has been identified as presenting the same cyber threat as Russia[88]). This also presents a substantially greater risk than companies with "offices" in Russia or China, since no detail is provided on whether sensitive activities occur at these offices, or whether they are limited to or focused on sales and marketing. Furthermore, companies with unspecified servers in Russia, China, or other countries are distinguishable from a company like Kaspersky that controls its servers from Russia and whose top leadership includes individuals with admitted ties to Russian government agencies).

ii. Vulnerabilities of Other Anti-Virus Software

BRG states that it "conducted a search of historical CVE [*i.e.*, Common Vulnerabilities and Exposures] data and other public vulnerability disclosures to evaluate the extent to which these products may have been (or have been) exploitable by malicious actors."[89] BRG's research identified what it characterizes as critical security vulnerabilities, publicly disclosed in the past five years, in anti-virus software from all seven companies (although, again, not necessarily in

[85] *See* BRG Assessment at 20-22.
[86] BRG identified 889 individuals in China who list Symantec as their employer on their LinkedIn profiles. *See* BRG Assessment at 22.
[87] Exhibit 6 (Kaspersky Lab, *Principles for the processing of user data by Kaspersky Lab security solutions and technologies*, https://usa kaspersky.com/about/data-protection).
[88] *See, e.g.,* Exhibit 4 (Information Memorandum at 7).
[89] BRG Assessment at 11.

the specific software product(s) used by federal agencies).[90] Kaspersky also notes that "BRG's review identified several instances in which hackers have been able to compromise some of the anti-virus companies themselves."[91]

DHS is aware of vulnerabilities identified in anti-virus products from Kaspersky and other developers. However, DHS's concern about Kaspersky products does not depend on any specific technical vulnerability(ies) that have been disclosed previously or that may be disclosed in the future. Rather, as explained above, it is the normal functioning of Kaspersky products, which is susceptible to exploitation by Russian actors, that creates the information security risks on which the BOD was issued.

iii. Data Collection by Other Anti-Virus Software

The Information Memorandum explained that Kaspersky customers who choose to participate in the Kaspersky Security Network ("KSN") must agree to a KSN Statement that authorizes the automated transfer of a lengthy list of sensitive data from the user's computer to the KSN.[92] As stated in Section II.A.2 above, Kaspersky's front-end KSN servers are located in various countries around the world, including Russia, and the data stored in the KSN is accessible by Kaspersky personnel located in Russia.

Kaspersky concedes that "if an end-user chooses to participate in the 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."[93] Kaspersky and BRG argue, however, that the End User License Agreement ("EULA") and/or Privacy Policy documents from the six other anti-virus software vendors to the U.S. government permit similar or broader data collection than Kaspersky.[94]

This discussion of other vendor data collection does not address DHS's concerns with the KSN Statement. DHS's concern with the KSN statement is not the collection of data for further analysis by anti-virus companies generally, or the fact that such companies may be permitted to transfer such data to third parties in other countries;[95] rather, DHS's specific concern with respect to the KSN statement relates to data collected or collectible by Russian actors, through these cloud-based systems, for malicious purposes, and neither BRG nor Kaspersky has presented evidence that any of these other vendor networks present a comparable risk to Kaspersky.

---

[90] *See* BRG Assessment at 10-16 (providing examples of the specific vulnerabilities).
[91] Kaspersky Submission at 11. Kaspersky appears to be referring to three items identified by BRG: (1) An unconfirmed New York Times report in October 2017 that "Israel had gained access to Kaspersky networks and identified NSA hacking tools"; (2) a September 2017 report by Cisco Talos security research division that "hackers had inserted a backdoor into CCleaner, an Avast-developed product intended to clean up devices"; and (3) a 2008 CNET report that Trend Micro's website (which is distinguishable from a compromise of internal IT resources) was hacked. *See* BRG Assessment at 12-13, 16.
[92] *See* Exhibit 4 (Information Memorandum at 6-7).
[93] Kaspersky Submission at 13.
[94] *See* Kaspersky Submission at 13-14; BRG Submission at 16-20.
[95] *See* Kaspersky Submission at 22; BRG Assessment at 21.

iv. Breadth of Presence on Federal Networks

Kaspersky explains that it has a relatively small presence on federal networks,[96] and it argues that the Russian Government would more effectively obtain sensitive U.S. government information by targeting a company with a larger presence on federal networks, such as Symantec and McAfee.[97]

First, as stated in the Information Memorandum, Russia is a full-scope cyber actor that DHS anticipates would use any available access to U.S. government information systems, including through Kaspersky anti-virus, and not hold back on exploiting Kaspersky's access because other anti-virus providers may have a larger installed base on federal networks.[98] This is particularly true because access to one device or network often can be used by sophisticated attackers to gain access to other devices and networks. In addition, the other anti-virus products that BRG reviewed are not subject to the full scope of risks arising under Russian law that arise with Kaspersky.

3. Information Security Risks of Other IT Products

The BRG Assessment briefly states that software products other than anti-virus software are potentially susceptible to exploitation by a malicious actor. For example, several applications commonly found on federal information systems, such as web browsers, Microsoft Office products, and the Microsoft Windows operating system, have "repeatedly been demonstrated to contain security vulnerabilities which could result in the execution of arbitrary code or commands on the victim's computer." Enterprise-level hardware products, including network firewalls, also "have been found to contain vulnerabilities that could be leveraged by a malicious actor to gain unauthorized access to data or systems."[99]

DHS agrees that software and hardware, other than Kaspersky anti-virus products, can present information security risks to federal networks. However, the interrelationship of factors upon which DHS's decision was based are not present — or present to a much lesser degree if at all — in other information security products. Moreover, as stated above with respect to anti-virus software written by other companies, DHS is under no requirement to address the information security risks presented by all information technology products when issuing a BOD. Instead, BOD 17-01 addresses a particularly acute set of risks presented by products of a specific company. DHS has authority to issue later BODs, or to exercise other authorities, to address other information security risks that other products present to federal networks as appropriate.

4. Suggested Framework for U.S. Government Software Procurement

The BRG Assessment concludes with a "Suggested Systematic Framework for U.S. Government Security Software Procurement."[100] As with BRG's "Preliminary Review" of Kaspersky

[96] *See* Kaspersky Submission at 7-8.
[97] *See* Kaspersky Submission at 16.
[98] Exhibit 4 (Information Memorandum at 7-8).
[99] BRG Assessment at 7.
[100] BRG Assessment at 33-35.

software, it is not clear whether Kaspersky supports this Suggested Systematic Framework because Kaspersky does not address it anywhere else in the Kaspersky Submission.

The Framework offered by BRG is an "outline" of "several key factors" that BRG believes should be considered "when reviewing a security-critical software product, such as anti-virus software, or vendor for use on federal information systems."[101] BRG suggests, for example, that federal agencies should (i) agree on a set of secure software development practices and require compliance with those practices and standards to qualify for government procurements; (ii) implement a consistent framework for assessing information security risk in a given software product; and (iii) ensure that software is deployed, configured, and updated appropriately.[102]

For purposes of this Information memorandum and BOD 17-01, DHS does not need to take a position on this Suggested Systematic Framework because the Suggested Systemic Framework is irrelevant to the question of whether Kaspersky-branded products present a known or reasonably suspected information security threat, vulnerability, or risk. Nevertheless, as you know, DHS and other federal agencies are constantly evaluating software procurement risks based on a range of factors. Furthermore, the NDAA discussed in Section II.B above requires a review and report by the Secretary of Defense, in consultation with the Secretary of Homeland Security and other agency heads, that addresses, among other topics, "Federal Government-wide authorities that may be used to prohibit, exclude, or prevent the use of suspect products or services on the information technology networks of the Federal Government."[103]

C. Kaspersky Legal Arguments

Kaspersky raises several legal challenges to the BOD and the accompanying administrative process. The company argues that DHS (i) deprived Kaspersky of Constitutional due process by ordering agencies to remove its products without giving the company prior notice and an opportunity to be heard, (ii) violated its Constitutional right to equal protection by failing to offer a rational basis for targeting Kaspersky alone, and (iii) acted in an arbitrary and capricious manner, abused its discretion, and issued the BOD without substantial evidence in violation of the Administrative Procedures Act ("APA").

I am confident that the BOD procedures are constitutional and lawful. DHS exercised its statutory authority to issue a BOD for purposes of safeguarding federal information and information systems from known or reasonably suspected threats, vulnerabilities, or risks. This was a sensitive and inherently discretionary judgment call, based on a substantial body of evidence and based on national security concerns. That evidence, to the extent it could be released, was disclosed to Kaspersky, and the process thus provided Kaspersky with meaningful notice and opportunity to confront the evidence against it, and the process used by DHS is analogous to other agency actions involving similar issues. In addition, the administrative record provides adequate support for your conclusion that Kaspersky-branded products present a known or reasonably suspected national security threat to federal information systems. Finally, DHS has

[101] BRG Assessment at 33.
[102] BRG Assessment at 34.
[103] Exhibit 3 (Excerpt from National Defense Authorization Act for Fiscal Year 2018, § 1634(c), https://www.congress.gov/115/bills/hr2810/BILLS-115hr2810enr.pdf).

acted appropriately to address information security risks presented specifically and uniquely by this company's products and services. Ultimately, I am convinced that the company's legal arguments are unfounded and the determination to issue the BOD was proper and consistent with the parameters in the U.S. Constitution, FISMA, and the APA.

IV. RECOMMENDATION

I have considered the totality of the administrative record. This includes the information security risks presented in the Information Memorandum, including the original NCCIC Assessment; the information and arguments presented by Kaspersky in the Kaspersky Submission, including the BRG Assessment; the NCCIC Supplemental Assessment prepared in response to the BRG Assessment; the analysis of relevant provisions in Russian law presented in the Maggs Report; the relationship between BOD 17-01 and the NDAA; and the information in this memorandum.

The record presents a compelling picture of the various ways that the Russian Government, and particularly the FSB intelligence agency, can compel, request, and otherwise exploit the access provided by Kaspersky-branded products to the information and information systems of Kaspersky customers, including U.S. government customers. This includes the general obligation for private entities like Kaspersky to assist the FSB in its intelligence, counterintelligence, and other broadly-defined duties, as well as more specific risks that Kaspersky will install equipment and software that permits monitoring of its network, provide decryption keys or other information to the FSB to enable clear-text access to encrypted transmissions, and provide other information to the FSB with or without the company's collaboration. Further, if Eugene Kaspersky consents, the FSB also is permitted to second FSB military personnel to Kaspersky offices, where such FSB personnel may have broad ability to view and collect customer data, send malware to customer computers, or other take other actions that present significant risks to federal information and information systems.

The NCCIC Supplemental Assessment also usefully examines the limitations of the assessment of Kaspersky software prepared by BRG. As NCCIC highlights, BRG confirms key aspects of the NCCIC Assessment, including the broad access to files and high-level privileges with which Kaspersky software operates. The specific testing that BRG has done to date also does not meaningfully address the information risks that NCCIC has identified. Specifically, BRG has not proven or even provided evidence that the FSB would be unable to monitor and decrypt traffic between Kaspersky's offices and Moscow and Kaspersky users (directly or through the KSN); that not participating in the KSN or deploying the Kaspersky Private Security Network prevents transmission of customer data to Kaspersky; or that a malicious cyber actor such as the FSB could not write signatures (*e.g.*, when on secondment to Kaspersky) or otherwise exploit the Kaspersky software to conduct targeted searches of customer computers and networks for specific information.

Based on all of this information, I maintain my recommendation that you determine that Kaspersky-branded products present known or reasonably suspected information security risks to federal information and information systems. These risks arise because of the broad access to files and high-level privileges of anti-virus software, including Kaspersky–branded products; the publicly-reported and Kaspersky-acknowledged ties between Kaspersky officials and the

Russian Government; and the significant authorities under Russian law, detailed in the Maggs Report, that permit the FSB to request or compel assistance from Kaspersky and to intercept transmissions between Kaspersky and its federal government customers without a court order. This recommendation is based upon expert judgments relating to national security. Classified information, provided in the Classified Annex to the Information Memorandum, further supports this recommendation.

In response to these concerns, Kaspersky has not submitted a clear and comprehensive proposal to mitigate these risks. Instead, Kaspersky suggests that agencies could use both Kaspersky software and anti-virus software from another vendor (to address the risk that Kaspersky or the Russian Government would intentionally withhold needed signature updates), and that agencies either could decline participation in the KSN or deploy the local KPSN. However, as described in the NCCIC Supplemental Assessment and Section III.A.2 above, use of multiple anti-virus products creates technical and budgetary issues while not addressing the key risks, declining participation in KSN does not eliminate transmission of data to Kaspersky, and neither declining participation in KSN nor deploying a local KPSN addresses the risks of malicious signature or software updates, which could impair the integrity or availability of federal information and information systems, among other information security risks. In sum, none of these options individually or collectively address the information security risks that necessitated issuance of BOD 17-01.

For the above reasons, I recommend that you issue a Final Decision that maintains BOD 17-01 without modification. As required by the administrative process that DHS made available to Kaspersky and other entities, I also recommend that you transmit a letter to Kaspersky enclosing the Final Decision, this Information memorandum, and its exhibits, including the NCCIC Supplemental Assessment and the Maggs Report.