Exhibit L

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.

Exhibit 1

REPORT OF PETER B. MAGGS

INTRODUCTION

1. I have been retained by the Department of Homeland Security to advise on Russian law.

2. In this capacity, I have reviewed the Information Memorandum from the Assistant Secretary for Cybersecurity and Communications to the Acting Secretary, dated September 1, 2017, and the Kaspersky Lab Request for Department of Homeland Security to Initiate Review of Binding Operational Directive 17-01.

3. I am providing this Report to be attached to a memorandum from the Assistant Secretary for Cybersecurity and Communications to the Secretary of Homeland Security. This Report is based on my review and analysis of Russian laws related to the authorities of Russian intelligence and other government agencies, to the requirements for private enterprises to develop, use, and sell products that use encryption, and to other matters relevant to Binding Operational Directive 17-01. This Report is not intended to be an exhaustive analysis. If needed for a future purpose, I may supplement this Report.

4. All translations in this report have been made or verified by me.

MY QUALIFICATIONS AND EXPERIENCE

5. I teach at the University of Illinois, where I am Professor of Law Emeritus and holder of the Clifford M. & Bette A. Carney Chair Emeritus. My specialty is law of the Russian Federation, law of the other former Soviet republics, and law of the former Soviet Union.

6. I have consulted on Soviet and Russian law for government agencies and for lawyers with clients investing in and trading with the USSR and, more recently, Russia and other former Soviet republics. I speak, read, and write Russian fluently, and I have visited Russia frequently.

7. I have studied law both in the United States and in Russia. In 1957, I received an A.B. Degree from Harvard College in Classics and Slavic and, in 1961, I received a J.D. Degree from Harvard Law School. During 1961-1962, I was an exchange post-graduate student at the Faculty of Law of Leningrad (now St. Petersburg) State University. There, I studied with Professor O.S. Ioffe, a leading expert on Russian civil law. In 1963-1964, I was an associate of the Harvard Russian Research Center and a Research Associate at Harvard Law School. In 1977, I taught as a Fulbright Lecturer at Moscow State University.

8. After the dissolution of the Soviet Union, I worked extensively under United States government auspices on foreign aid projects designed to help with the creation of the legal basis for a market economy in the Russian Federation and the other former Soviet republics. One important part of this effort was the creation of model Civil Code legislation, which eventually became a basis for the civil codes of a number of former republics. In connection with this project, I met frequently with civil code drafters from Russia and other former republics during the 1990s.

9. I am 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 and a book, Law and Legal System of the Russian Federation, which I co-authored with Professor William Burnham, Olga Schwartz, and the late Professor Gennady M. Danilenko. In addition to my writings on Russian law, I am also the co-author of several casebooks and the author of various articles on United States law.

10. An up-to-date copy of my curriculum vitae is attached as Appendix 1 to this Report.

THE RUSSIAN LEGAL SYSTEM

Introduction

11. The Russian legal system belongs to the European civil law family (or continental system). Russian law makes a strict division between different branches of law, such as criminal law, civil law, and labor law. Each branch has its own principles and sources of legislation. Usually the key principles of each branch are codified, for instance in the Civil Code and the Civil Procedure Code. The system of Russian law and of Russian civil law, in particular, is much more closely related to German law than to French law. However, it would be a great mistake to assume that any rule or the interpretation of any legal provision in Russia would necessarily follow the law in other civil law countries.

Sources of Law

12. The principal sources of the law of the Russian Federation, in hierarchical order, are: the Constitution of the Russian Federation, laws adopted by the Russian Parliament, decrees of the President, and regulations issued by the Government and governmental agencies. There is also legislation adopted at regional and city levels, but this legislation is not relevant to the legal issues discussed in this Report. When ordinary laws in a particular branch are changed, generally the codes are changed at the same time to avoid conflicts.

Statutes often contain cross-references clarifying their relationship to various branches of law.

SUMMARY OF LEGAL ANALYSIS

13. Below I provide a summary of my legal analysis. My conclusions are as follows:

(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 Lab.

(b) Private enterprises, including Kaspersky Lab, 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 Lab, 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 Lab 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 implement other means that enable the FSB and potentially other state authorities to monitor data transmissions between Kaspersky's computers in Russia and Kaspersky Lab customers.

(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 Lab is obliged to assist the FSB with such operational-investigative activities.

(f) Kaspersky Lab 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 Lab's encrypted data transmissions.

DETAILED LEGAL ANALYSIS

(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 Lab.

14. The Federal Law of April 3, 1995, No. 40-FZ, "On the Federal Security Service" requires FSB bodies to carry out their activities in collaboration with various entities in Russia, including private enterprises such as Kaspersky. This obligation is stated in the first paragraph of Article 15 of this law:

> Federal security service bodies shall carry out their activity in collaboration with federal bodies of state authority, bodies of state authority of constituent entities of the Russian Federation, enterprises, institutions, and organizations, regardless of their form of ownership.

15. The "bodies" of the FSB are defined in Article 2 of the same law as the "federal body of executive authority in the area of ensuring security" and the regional and specialized security bodies subordinate to it.

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

16. The Federal Law of April 3, 1995, No. 40-FZ, "On the Federal Security Service" places private enterprises under a legal obligation to assist FSB bodies in the execution of the duties assigned to the FSB bodies. This obligation is stated in the third paragraph of Article 15 of this law:

> State bodies and also enterprises, institutions and organizations have the obligation to assist federal security service bodies in the execution of the duties assigned to these bodies.

17. The duties assigned to these bodies may be in any of the "basic directions" listed in Article 8 of the Law 40-FZ of April 3, 1995, as amended, which provides:

> **Article 8. Directions of Activity of the Federal Security Service Bodies**
>
> The activity of federal security service bodies shall be conducted in the following basic directions:
>
> counterintelligence activity;
>
> the fight with terrorism;
>
> the fight with crime;

intelligence activity;

border activity;

ensuring information security.

Other directions of activity of federal security service bodies shall be defined by federal legislation.

18. In particular, Kaspersky Lab must assist FSB bodies in their counterintelligence and intelligence activity, since these are duties assigned to FSB bodies. These activities are defined in the first paragraph of Article 9 and the first paragraph of Article 11 of the Federal Law of April 3, 1995, No. 40-FZ, "On the Federal Security Service":

Article 9. Counterintelligence Activity

Counterintelligence activity – activity conducted by bodies of the federal security service and/or their subdivisions (hereinafter in this Article – "counterintelligence bodies"), and also by official persons of these bodies and subdivision by the conduct of counterintelligence measures for the purpose of revealing, preventing, and stopping intelligence and other activity of special services and organizations of foreign states and also of individual persons, which is directed at causing harm to the security of the Russian Federation.

Article 11. Intelligence Activity

Intelligence activity is conducted by the body of foreign intelligence of the federal body of executive activity in accordance with the Federal law "On Foreign Intelligence."

The manner of interaction of the body of foreign intelligence of executive authority in the area of ensuring security with other bodies of foreign intelligence of the Russian Federation is defined by federal legislation and by agreements concluded among them, and/or by joint normative legal acts.

The manner of conducting intelligence measures and the manner of use of special methods and means in the conduct of intelligence activities shall be established by normative legal acts of the federal body of executive authority in the area of ensuring security.

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

19. As appears from Article 7 of the Federal Law of April 3, 1995, No. 40-FZ, "On the Federal Security Service," the Federal Security Service has its own military service personnel, in addition to civil service personnel, and ordinary employees.

20. The Federal Law of April 3, 1995, No. 40-FZ, "On the Federal Security Service" permits FSB military service personnel to be seconded to private enterprises, including Kaspersky, with the consent of the head of the enterprise and with the FSB military service personnel remaining on military service during the secondment. This authority is stated in the sixth paragraph of Article 15 of this law:

> For the purposes of resolving the tasks of safeguarding the security of the Russian Federation, military service personnel of federal security service bodies may be seconded to state authorities, enterprises, institutions and organizations, regardless of their form of ownership, with the consent of their heads and in the manner established by the President of the Russian Federation, while remaining on military service.

(d) Kaspersky Lab 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 implement other means that enable the FSB and potentially other state authorities to monitor data transmissions between Kaspersky's computers in Russia and Kaspersky Lab customers.

21. Article 10.1 (introduced by the Federal Law of May 5, 2014, No. 97-FZ) of the Federal Law of July 27, 2006, No. 149-FZ, "On Information, Information Technologies, and Protection of Information," places a number of important obligations on any entity that qualifies as "an organizer of the dissemination of information on the Internet" as defined in the Law. The term "organizer of the dissemination of information on the Internet" is defined in Article 10.1.1 as follows:

> An organizer of the dissemination of information on the Internet is a person who carries out activities to ensure the operation of information systems and/or programs for electronic computers that are designed and/or used to receive, transmit, deliver and/or process electronic messages of users of the Internet.

22. Kaspersky Lab qualifies as "an organizer of the dissemination of information on the Internet" because its anti-virus software carries out activities to ensure the operation of information systems and are designed and used to receive, transmit, deliver, and process

electronic messages, including data transmissions and emails, between Internet users (i.e., Kaspersky Lab and its customers).

23. The duties of organizers of the dissemination of information on the Internet are stated in Paragraphs 2 through 4.1 of Article 10.1, which are currently in effect except as noted, and which provide:

> **Article 10.1. The Duties of the Organizer of the Dissemination of Information on the Internet**
>
> 2. An organizer of the dissemination of information on the Internet network is obliged to notify the federal executive body that performs functions of control and supervision in the sphere of mass media, mass communications, information technologies and communications in accordance with the procedure established by the Government of the Russian Federation, of the initiation of activities specified in part 1 of this Article.
>
> 3. An organizer of the dissemination of information on the Internet network is obliged to keep on the territory of the Russian Federation:
>
> 1) information about the receipt, transmission, delivery and/or processing of voice information, written text, images, sounds, video or other electronic messages of users of the Internet and information about these users within one year from the end of the implementation of such actions;
>
> ***Subparagraph 2 immediately below takes effect July 1, 2018***
>
> *2) text messages of Internet users, voice information, images, sounds, video, other electronic messages of Internet users up to six months from the end of their reception, transmission, delivery and/or processing. The procedure, terms and volume of storage of information specified in this subparagraph shall be established by the Government of the Russian Federation.*
>
> 3.1. The organizer of the dissemination of information on the Internet network is obligated to provide information specified in Point (3) of this Article to

authorized state bodies carrying out operational-investigative activity or ensuring the security of the Russian Federation in cases stipulated by federal laws.

[An amendment effective January 1, 2018, changed the words "Point 3" above to "Part 3".]

4. An organizer of the dissemination of information on the Internet shall have the duty to ensure the implementation of the requirements for the equipment and for the technical and program means used by the organizer in the operation by it of information systems, i.e., the requirements that have been established by the federal body of executive power in the area of communications by agreement with the authorized state bodies conducting operative search activity or ensuring security of the Russian Federation for use by the conduct by these bodies (in cases provided by federal laws) of measures for the purposes of carrying out the tasks assigned to these bodies. The organizer also shall have the duty to take measures to prevent the discovery of the organizational and tactical methods of the conduct of such measures. The Government of the Russian Federation shall establish the manner in which the organizers of the distribution of information on the Internet interact with the authorized state bodies conducting operative-search activity or ensuring the security of the Russian Federation.

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

24. An important way in which the FSB carries out its duties is by "operational-investigative activities." Such activities are governed by Federal Law No. 144-FZ of August 12, 1995 (as amended), "On Operational-Investigative Activity."

25. Article 6 of the Federal Law of August 12, 1995, No. 144-FZ, as amended through July 6, 2016, "On Operational-Search Activity" requires private businesses, including Kaspersky Lab, to install any equipment supplied by the FSB for use in obtaining computer information.

Article 6. Operational-Search Measures

The following operational-search measures are conducted in the conduct of operational search activity:

. . .

15. Obtaining computer information.

. . .

Operational-search measures connected with the monitoring of things sent by post, telegraph and other communications, eavesdropping on telephone conversations with connection to fixed apparatus of enterprises, institutions and organizations regardless of the form of ownership, and of physical and legal persons providing services and means of communication with the taking of information from technical channels of communications and with the receipt of computer information shall be conducted with the use of the operational-technical abilities and means of bodies of the federal security service and bodies of internal affairs in the manner determined by interdepartmental normative acts or by agreements among bodies conducting operational search activity.

. . .

26. The second paragraph of Article 8 of this Law makes it clear that, as a general rule, operational-investigative activities may be carried out against anyone anywhere:

> Citizenship, nationality, sex, place of residence, property, official or social status, membership in public associations, attitude toward religions and political views of individual persons are not a hindrance to the conduct of operational-investigative activities with respect to them unless otherwise provided by a federal law.

27. The third paragraph of Article 8 of this Law makes it clear that operational-search activities include obtaining computer information. This third paragraph also indicates that a court order is required if the activities affect constitutional rights, and that such court order may be issued only if one of the three listed grounds is present:

> Carrying out operational-search activities (including obtaining computer information) which restrict the constitutional rights of man and the citizen to the secrecy of correspondence, telephone conversations, postal, telegraphic and other messages transmitted over electric and postal communication networks, as well as the right to inviolability of the home, is allowed on the basis of a court decision and in the presence of information:
>
> 1. On the signs of a prepared, committed or committed unlawful act, according to which the production of the preliminary investigation is

mandatory.

2. On persons who prepare, commit or have committed a wrongful act, according to which the production of the preliminary investigation is mandatory.

3. On events or actions (inaction) creating a threat to the state, military, economic, information or environmental security of the Russian Federation.

28. The fourth paragraph of Article 8 allows a 48-hour period of operational-search activities without a court order, even if the activities affect citizen's constitutional rights:

> In cases that do not tolerate delay and can lead to the commission of a grave or especially grave crime, and also in the presence of data on events and actions (or inaction) creating a threat to the state, military, economic, information or ecological security of the Russian Federation, on the basis of a reasoned decision one of the heads of the body that carries out operational-search activity it is allowed to conduct the operational-search activities, provided by part two of this Article, with the obligation of informing a court (or judge) within 24 hours. Within 48 hours from the moment of the beginning of the operational-search activity, the body that implements it is obliged to obtain a court decision on carrying out such an operative-investigative measure or to stop it.
>
> . . .

29. It is important to note that the restrictions in the third paragraph of Article 8, which require a court order for monitoring or intercepting private communications, are limited to communications involving rights of privacy of communication guaranteed to private individuals by the Constitution of the Russian Federation. Nothing in these restrictions indicates that they protect the secrecy of (1) the content of computers owned or used by the United States government for government-related purposes; (2) communications between individuals not subject to Russian constitutional guarantees, such as private communications outside Russia between individuals who are not Russian citizens; or (3) personal information about people outside Russia who are not Russian citizens. Therefore, operational-investigative activity by the FSB to collect any of these three types of information does not require a court order.

30. In sum, Kaspersky Lab's legal obligation to assist the FSB in its counterintelligence and intelligence functions includes a duty to assist the FSB in operational-investigative activity,

in support of FSB counterintelligence and intelligence functions in the situations listed above (e.g., collecting information from U.S. computers), with no need for the FSB to have obtained a court order.

(f) Kaspersky Lab 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 Lab's encrypted data transmissions.

31. Paragraph 4.1 of Article 10.1 of the Federal Law of July 27, 2006, No. 149-FZ, "On Information, Information Technologies, and Protection of Information," requires Kaspersky 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 communications. Article 10.1 was added to this law by the Federal Law of May 5, 2014, No. 97-FZ. Paragraph 4.1 was added to Article 10.1 by the Federal Law of July 6, 2016, No. 374-FZ. Paragraph 4.1 reads as follows:

> **Article 10.1. The duties of the organizer of the dissemination of information on the Internet**
>
> . . .
>
> 4.1. The organizer of the dissemination of information on the Internet network is obliged when using additional electronic message coding for receiving, transmitting, delivering and/or processing electronic messages of Internet users and/or when providing Internet users with the possibility of additional coding of electronic messages, to present to the federal executive body in the field of security the information necessary to decode the received, transmitted, delivered and/or processed electronic communications.

COMMENTS ON THE KASPERSKY LAB REQUEST FOR REVIEW

32. I have been supplied with a copy of the "Kaspersky Lab Request for Department of Homeland Security to Initiate Review of Binding 5. Directive - 17-01" and have been asked to comment on some of the assertions concerning Russian law and Russian legal obligations on pages 19-22 of the Request.

33. The short summary of the duties of the FSB on page 19 is correct.

34. Later on page 19, Kaspersky also accurately states that the FSB can request information from companies in Russia in furtherance of the FSB's duties and that such companies are obligated to comply with the request. However, Kaspersky states on page 19 that "the

FSB's powers in this regard are not unlimited, and FSB requests are subject to challenge in court." I have searched the leading Russian legal database, "Consultant Plus", for cases involving the power given to the FSB to require state agencies and private businesses "to assist federal security service bodies in the execution of the duties assigned to these bodies". I found only two such cases. Neither case was brought against the FSB. Rather both cases were brought against parties sanctioned by public authorities. These parties complained that various entities had improperly voluntarily cooperated with the FSB. The complaints of both parties were rejected.

35. In one case, a private company complained that other organizations had improperly cooperated with the FSB in helping to find information on the basis of which the private company was fined.[1]

36. In another, a regional public entity was sanctioned by the Federal agency that enforced public contract bidding legislation. The Federal agency had acted on the basis of information of violation of the legislation provided to it by the FSB. The regional public entity argued that the Federal agency should not have acted on this basis. The court upheld the actions of the Federal agency in acting on the basis of the FSB information. The court noted that "the list of matters on which state bodies, enterprises, and institutions regardless of form of ownership were obligated to render aid to security bodies was rather broad."[2]

37. This statement confirms my opinion that, while the FSB's powers are not "unlimited," the FSB's duties are very broadly written and interpreted.

38. Thus my research revealed not a single case brought against the FSB by a party seeking to avoid cooperation with the FSB.

39. I have not conducted detailed research and analysis on the specific requirements and processes for obtaining licenses and certificates related to encryption products in the Russian Federation. However, based on the materials that I have reviewed, I generally agree that one or more components of the FSB are involved in granting encryption-related licenses to companies and that the U.S. Department of the Treasury, Office of Foreign Assets Control has issued a general license to authorize certain otherwise-prohibited transactions with the FSB.

40. On page 21, Kaspersky Lab states that Kaspersky Lab and Military Unit 43753 are separate organizations, and Kaspersky Lab attaches as exhibits English-language translations of the

[1] Decision of the Twenty-first Arbitrazh Appellate Court of July 21, 2017, No. AP-1382/2017 in Case No. A83-3691/2017.
[2] Decision of the Twelfth Arbitrazh Appellate Court of March 18, 2015, No. 12AP-581/2015 in Case No. A06-7963/2014,

Russian Trade Register for each organization. I found the same registration records by searching the Russian tax service's public online corporate registry. However, the discussion on page 21 fails to explain the nature of the relationship between Kaspersky Lab and Military Unit 43753 that led to the joint issuance of the certificates in 2007 and 2011. I note that the Kaspersky Request states [emphasis added]:

> 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.

41. I would expect that Kaspersky Lab's files would contain documentation that provides actual evidence of the relationship between Kaspersky Lab and Military Unit 43753 connected with the joint issuance of the certificates. Apparently the authors of the Request either were not given access to this documentation or chose not to address further in the Request. Rather, Kaspersky Lab only states what "presumably" might have occurred.

42. The most problematic portion of the discussion of Russian law in the Request is in its discussion (pages 21-22) of Russian legislation on operative-investigative measures.

43. The Request states:

> 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"). 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").

44. The above statement is incorrect. First, as explained in subsection (e) above, the FSB has long had the power to engage in operational-investigative measures and Kaspersky Lab has long had the duty to cooperate with such measures. As explained above in paragraph 25, this duty would include the installation of any special equipment provided by the FSB.

45. Second, as also explained in subsection (d) above , Kaspersky Lab has the duty as an "organizer of the disseminator of information on the Internet" to install hardware or software that permits FSB monitoring and interception of data transmissions between

Kaspersky and its customers. These laws and tools apply to Kaspersky Lab whether or not it is considered to be a provider of communications services.

46. Further, the Request's statement, "Kaspersky Lab does not provide communication services, thus the Company is not subject to these laws or other government tools[,]" is quite dubious.

47. Article 15 of Law 40-FZ of April 3, 1995, "On the Federal Security Services," has provided ever since its enactment in 1995, in what is now its fifth paragraph (emphasis added):

> Physical persons and legal entities in the Russian Federation providing postal communications services and ***electronic communications services of all types***, including data, confidential, and satellite communications systems, ***shall be under obligation, at the request of federal security service bodies, to include in the apparatus additional hardware and software and create other conditions required to implement operational/technical measures by bodies of the federal security service***.

48. To interpret the meaning of "legal entities . . . providing . . . electronic communications services of all types," it is common practice in interpreting Russian legislation to use the definition of terms in the main law in a particular area to interpret the meaning of terms in other laws that use these terms. Terms concerning communications were defined in Law No. 15-FZ of February 16, 1995, "On Communications." These definitions would have been, and still are, used to interpret the meaning of identical or almost identical terms used in Law No. 40-FZ of April 3, 1995, "On the Federal Security Service." Thus, to interpret the scope of "legal entities . . . providing . . . electronic communications services of all types," I researched and identified the following relevant definitions in Law No. 15-FZ of February 16, 1995, "On Communications" [emphasis added]:

> **Article 2. Basic Terms Used in the Present Federal Law**
> For the purposes of the present Federal Law, the following basic terms are used:
>
> Electrical communications (electronic communications) – every transmission or receipt of signs, signals, written text, images, or sounds over cable, radio, optical or other electromagnetic systems;
>
> . . .
>
> Electronic communications networks – technological systems providing one or several types of transmissions: telephone, telegraph, fax, transfer of data and other types of documentary communications, ***including exchange of information among computers,*** television, sound and other types of radio and cable broadcasting;

49. The 1995 Law on Communications was repealed and replaced by Federal Law No. 126-FZ of July 7, 2003, "On Communications." This law had a somewhat different list of definitions. As stated in paragraph 48 above, Russian practice has been to interpret terms in one law using definitions for the same or similar terms at the time the borrowing legislation was passed. Thus, the definitions in the 1995 Law On Communications are the relevant definitions when interpreting paragraph 5 of Article 15 of Law 40-FZ of April 3, 1995, "On the Federal Security Services." Although, in my opinion, the definitions in the 2003 Law are not relevant, I nevertheless provide them immediately below:

> **Article 2. Basic Terms Used in the Present Federal Law**
>
> For the purposes of the present Federal Law the following basic terms are used:
>
> . . .
>
> 24) communications network – a technological system including means and lines of communications and meant for electronic communications or postal communications;
>
> . . .
>
> 35) electronic communications – any emission, transfer, or receipt of symbols, signals, voice information, written text, images, sounds or communications of any type by a radio system, cable, optical or other electromagnetic systems;

50. Using the definitions in the 1995 Law, Kaspersky Lab certainly is engaged in the "transmission or receipt" of signals and certainly has set up a world-wide system that provides for the "transfer of data" and the "exchange of information among computers". Kaspersky Lab similarly provides electronic communications services under the definitions in the 2003 Law.

51. Thus, the FSB would have strong grounds to assert that under Article 15 of the Law on the FSB, Kaspersky Lab has the obligation, if requested, to "include in the apparatus additional hardware and software and create other conditions required to implement operational/technical measures by bodies of the federal security service."

52. In sum, apart from whether Kaspersky is subject to the requirement that telecom companies and ISPs install SORM equipment that permits surveillance of communications and data transmissions over telecom and ISP networks in Russia, Kaspersky Lab clearly is subject to "other government tools" that raise significant risks that Kaspersky Lab will be required

or requested to cooperate with FSB intelligence and other activities. For instance, the FSB could require that Kaspersky Lab install monitoring equipment provided by the FSB.

53. Whether or not the FSB has requested that Kaspersky Lab cooperate by installing monitoring equipment, Kaspersky Lab concedes that "[e]ncrypted 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." Kaspersky then does not deny that its data transmissions with customers occur using the networks of Russian telecom providers or Russian ISPs.

54. The Request goes on to state:

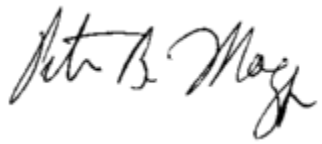
> However, the FSB is only legally permitted to use SORM in a limited number of situations and each use of SORM technology is subject to court oversight. Law enforcement officers wishing to use this technology must obtain a prior court order in each case when the technology is to be used against a particular person or legal entity.

55. As pointed out in paragraphs 29-30 above, this statement is incorrect. The legal safeguards cited in the Request only apply to situations involving the privacy of personal communications protected by the Constitution of the Russian Federation. Communications sent from or received by United States government computers concerning United States government functions are not protected by the Russian Constitution. Therefore, I do not believe that the FSB would need to obtain any court order to use SORM technologies to intercept data transmissions between Kaspersky Lab and its U.S. government customers. In addition, as stated in paragraph 31 above, Kaspersky Lab 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 communications.

56. As explained above in paragraphs 21-23, starting July 1, 2018, internet service providers and other "organizers of the dissemination of information on the Internet" will be required to store all communications for six months. The FSB would have access to this data in carrying out its operational-search activity. And as explained in paragraphs 29-30 and 55

above, it would need no court order to access data other than private communications of Russian citizens.

Respectfully submitted,



Peter B. Maggs Date: December 2, 2017

APPENDIX 1 – CURRICULUM VITAE OF PETER B. MAGGS

Peter B. Maggs -- Biographical Information

Office Address:

University of Illinois College of Law, 504 East Pennsylvania Avenue, Champaign, Illinois 61820, USA

Telephones: office: (217) 333-6711, mobile: (202) 413-3213

Fax: (217) 244-1478

Email: p-maggs @ illinois.edu.

Homepage: http://www.illinois.edu/ph/www/p-maggs

Employment:

Professor of Law and Clifford M. and Bette A. Carney Chair Emeritus, University of Illinois at Urbana-Champaign, 2014-

Professor of Law, Clifford M. and Bette A. Carney Chair in Law, University of Illinois at Urbana-Champaign, 2002-2014.

Peer & Sarah Pedersen Professor of Law, University of Illinois at Urbana-Champaign, 1998-2002.

Richard W. & Marie L. Corman Professor of Law, University of Illinois at Urbana-Champaign, 1988-1998.

Acting Dean, College of Law, University of Illinois at Urbana-Champaign, fall 1990.

Professor of Law, University of Illinois at Urbana-Champaign, 1969-1988.

Associate Professor of Law, University of Illinois at Urbana-Champaign, 1967-69.

Assistant Professor of Law, University of Illinois at Urbana-Champaign, 1964-67.

Associate, Harvard Russian Research Center and Research Associate, Harvard Law School, 1963-64.

Fellowships, Visiting Appointments, etc.:

Summer 2004. Worked in Serbia for National Center for State Courts evaluating legal education and designing a program for assistance to law schools. Visited law schools, wrote extensive report

Winter 2002-2003. Worked in Russia for USAID evaluating legal education and designing programs for assistance to legal education. Visited law schools, participated in writing extensive report.

Spring Semester 2002. Fulbright Distinguished Chair, University of Trento, Italy.

Summer 2001. Fulbright Senior Scholar, University of Malaya, Petaling Jaya, Malaysia

Spring 1998 - Visiting Professor, George Washington University Law School

January 1995 - present. Consultant for USAID contractors and the World Bank on numerous law reform projects in the former USSR, including legislative drafting and legal education projects in Armenia, Belarus, Moldova, Kazakstan, Kyrgyzstan, Russia, Tajikistan, and Ukraine.

1995-2000; 2005-2015. - Member, Panel of Recommended Arbitrators, International Commercial Arbitration Court of the Russian Chamber of Commerce and Industry

2015-2018 – Panelist of the Kuala Lumpur Regional Centre for Arbitration

January 1994 - January 1995. On leave from the University of Illinois to serve as Director/Legal Reform Specialist for the Rule of Law Consortium, Washington, D.C., administering a contract from the United States Agency for International Development to support the "rule of law" in the newly independent states of the former Soviet Union.

Fulbright, Lecturer, Universidade Federal de Santa Catarina, Florianopolis, Brazil, May-August 1982.

Guggenheim Fellow, January-December 1979.

Fulbright Lecturer, Moscow State University, Spring Semester, 1977.

ACLS - Soviet Academy of Sciences Exchange Scholar, Novosibirsk, USSR, August 1972.

Senior Fellow, East-West Population Institute, Honolulu, Hawaii, Spring Semester 1972.

ACLS Summer Language Fellowship, Rumania, June-August 1969.

IUCTG Exchange Scholar, Bulgarian Academy of Sciences, Sofia, Bulgaria, June-August 1967.

Fulbright Scholar, Belgrade University, Belgrade, Yugoslavia, January-June 1967.

IUCTG Exchange Student, Leningrad State University [now St. Petersburg State University], Leningrad, USSR, September 1961 - June 1962.

Education:

A.B., Harvard College, 1957; J.D., Harvard Law School, 1961.

Subjects Taught:

Contracts; Sales, Copyright, Trademark & Unfair Competition, Statutory Interpretation, Russian Law.

Foreign Languages:

Fluent in Russian; good in Portuguese, competent in French; reading knowledge of German, Serbian, Bosnian & Croatian; Bulgarian; Macedonian; Ukrainian; Italian; Spanish; Romanian & "Moldovan".

Major Funded Research Projects Completed:

The Process of Making and Implementing Laws in the Soviet Union in the Gorbachev and Brezhnev Periods, under a contract with the U.S. Department of State, 1988-1989.

Soviet Law Under Gorbachev, under a contract with the U.S. Department of State, 1987-1988.

The Soviet Economy: A Legal Analysis, supported by the National Council for Soviet and East European Research, 1985-1986.

Soviet and East European Law and the Scientific and Technical Revolution, supported by the National council for Soviet and East European Research, 1979-1981.

Talking Computer Terminals for the Blind, supported by the U.S. Department of Health, Education, and Welfare, 1978- 1979, 1980-1981.

Soviet Law Under Khrushchev and Brezhnev, supported by the Ford Foundation, 1975-1978.

Computer-Based Legal Education, supported by the Council of Legal Education for Professional Responsibility, 1973-1975.

Miscellaneous:

Member, Board of Directors, Open Voting Consortium, <http://www.openvotingconsortium.org>, 2004-2006.

Member, Practicing Law Institute Advisory Committee on Intellectual Property Law, 1996-present.
Member, American Law Institute, Members Consultative Group on Uniform Commercial Code, Articles 2 (Sales), 2A (Leases), and 2B (Licenses), 1996-2003.

Member, American Law Institute Members Consultative Group on Intellectual Property: Principles Governing Jurisdiction, Choice of Law, and Judgments in Transnational Disputes,

2004-present.

Member, Board of Editors, The Uppsala Yearbook of East European Law, 2004-present.

Member, Board of Advisors, Central and East European Legal Materials, 1990-present.

Corresponding Member, International Academy of Comparative Law, 1988-present.

Member, American Law Institute, Members Consultative Group on Restatement of the Law, Third, Unfair Competition, 1987-1995.

Member, American Law Institute, 1986-present.

Member, Subcommission on Law, American Council of Learned Societies--USSR Academy of Sciences Commission on the Humanities and Social Sciences, 1986-1989.

Member, Board of Directors, Center for Computer-Assisted Legal Instruction, 1982-1985.

Parliamentarian, American Association for the Advancement of Slavic Studies, 1978-1983.

Editor, Soviet Statutes and Decisions, 1976-1984.

Consultant on Computer Systems, U.S. Department of Justice, 1979-1981.

Chairman, Committee on Soviet Law, American Bar Association Section of International Law, 1975-1981.

Co-Editor-in-Chief, Bulletin on Current Research in Soviet and East European Law, 1974-1981.

Chairperson, Section of Comparative Law, Association of American Law Schools, 1976-1977.

Member, Advisory Committee on Research on Law and Computer Technology, American Bar Foundation, 1975-1977.

Reporter, Uniform Land Transaction and Uniform Simplification of Land Transfers Act, National Council of Commissioners on Uniform State Laws, January 1974 - August 1976.

Guide, American National Exhibition, Moscow, summer 1959; awarded Medal of Merit of United States Information Agency.

Admitted to practice in the District of Columbia.

Peter B. Maggs -- List of Publications

Books

Translator and editor (with cotranslator and coeditor Alexei Zhilstov), *Civil Code of the Russian Federation as Amended through February 7, 2017* (with introduction by Olga Kozyr, Peter Maggs, and Alexei Zhiltsov). Book version: Createspace, 2017. Electronic Version: Kindle, 2017.

Translator and editor (with cotranslator and coeditor Alexei Zhilstov), *Civil Code of the Russian Federation, First Part, as of May 23, 2016* (with introduction by Olga Kozyr, Peter Maggs, and Alexei Zhiltsov). Book version: Createspace, 2016. Electronic Version: Kindle, 2016.

Translator and editor (with cotranslator and coeditor Alexei Zhilstov), *Civil Code of the Russian Federation, First Part, as of January 31, 2016* (with introduction by Olga Kozyr, Peter Maggs, and Alexei Zhiltsov). Book version: Createspace, 2016. Electronic Version: Kindle, 2016.

(with coauthors Olga Schwartz, William Burnham and the late Gennady Danilenko), *Law and Legal System of the Russian Federation*, 6th Ed. (Huntington, N.Y.: Juris Publishing, 2015).

(with coauthors John Soma and the late James Sprowl, *Computer and Internet Law*, 4th ed. (St. Paul, Minn.: West 2013).

(with coauthor Roger Schechter), *Trademark and Unfair Competition, Cases and Comments*, 7th ed. (St. Paul, Minn.: West, 2012).

(with coauthors William Burnham and the late Gennady Danilenko), *Law and Legal System of the Russian Federation*, 5th Ed. (Huntington, N.Y.: Juris Publishing, 2012).

Author of the introduction and translator, *Kazakhstan Law on Joint-Stock Company* (2012). This book is published in three forms: electronic for the Amazon Kindle, electronic for Barnes & Noble Nook, and paperback by Createspace. The paperback version has the English translation and Russian text of the law on parallel pages.

Translator and editor (with cotranslator and coeditor Alexei Zhilstov), *Civil Code of the Russian Federation, First Part* (in parallel official Russian text and English translation by Peter B. Maggs and Alexei Zhiltsov, with introduction by Olga Kozyr, Peter Maggs, and Alexei Zhiltsov). (Moscow & Berlin: Infotropic, 2010).

Translator and editor (with cotranslator and coeditor Alexei Zhilstov), *Civil Code of the Russian Federation, Second Part* (in parallel official Russian text and English translation by Peter B. Maggs and Alexei Zhiltsov) (Moscow & Berlin: Infotropic, 2010).

Translator and editor (with cotranslator and coeditor Alexei Zhilstov), *Civil Code of the Russian Federation, Third Part* (in parallel official Russian text and English translation by Peter B. Maggs and Alexei Zhiltsov) (Moscow & Berlin: Infotropic, 2010).

Translator and editor (with cotranslator and coeditor Alexei Zhilstov), *Civil Code of the Russian Federation, Fourth Part* (in parallel official Russian text and English translation by Peter B. Maggs and Alexei Zhiltsov) (Moscow & Berlin: Infotropic, 2010).

(with coauthors James Sprowl and John Soma) *Internet and Computer Law: Cases – Comments – Questions*, 3rd ed. (St. Paul: West, 2010.

(with coauthors James Sprowl and John Soma) *Teacher's Manual to Internet and Computer Law: Cases – Comments – Questions, 3rd ed.* (St. Paul: West, 2010.

(with coauthors William Burnham and Gennady Danilenko), Law and Legal System of the Russian Federation, 4th Ed. (Huntington, N.Y.: Juris Publishing, 2009).

Translator and editor (with cotranslator and coeditor Alexei Zhilstov) *Civil Code of the Russian Federation, Fourth Part* (in parallel official Russian text and English translation by Peter B. Maggs and Alexei Zhiltsov, with introductions by Alexander Makovsky and Peter Maggs), (Moscow: Wolters-Kluwer, 2008).

(with coauthors John Soma and James Sprowl) *Internet and Computer Law: Cases--Comments--Questions*, 2nd ed. (St. Paul: West Group, 2005).

(with coauthors William Burnham and Gennady Danilenko), Law and Legal System of the Russian Federation, 3rd Ed. (Huntington, N.Y.: Juris Publishing, 2004).

Translator and editor (with cotranslator and coeditor Alexei Zhiltsov), *Civil Code of the Russian Federation: Parallel Russian and English Texts* (Moscow: Norma, 2003).

(with coauthor Roger Schechter), *Teacher's Manual for Use With Trademark and Unfair Competition, Cases and Comments*, 6th ed. (St. Paul, Minn.: West Group, 2003).

(with coauthors John Soma and James Sprowl) *2002 Supplement to Internet and Computer Law: Cases--Comments--Questions* (St. Paul: West Group, 2002).

Translator and editor, *The Civil Code of the Russian Federation, Third Part* (Armonk, N.Y.: M.E. Sharpe, (2002).

(with coauthor Roger Schechter), *Trademark and Unfair Competition, Cases and Comments*, 6th ed. (St. Paul, Minn.: West Group, 2002).

(with John Soma and James Sprowl) *Teacher's Manual to Accompany Internet and Computer Law: Cases--Comments--Questions* (St. Paul: West Group, 2001).

(with John Soma and James Sprowl) *Internet and Computer Law: Cases--Comments--Questions* (St. Paul: West Group, 2001).

(with A.P. Sergeev) *Intelektual'naia sobstvennost'* ("Intellectual Property") (Moscow: Iurist, 2000). Also published on the Internet by the Open Society Institute (Moscow) (supported by the Soros Foundation) at: <http://www.auditorium.ru/books/343/.

Copyright / Statutory Interpretation (Teaching Materials) (Champaign: University of Illinois College of Law, 1998, 1999, 2001)

Translator (with Anna Tarassova and Alexei Zhiltsov) and editor (with Vladimir Nazaryan and Anna Tarassova), *Civil Code of the Republic of Armenia* (Yerevan: Iris, 1999). Published on the Internet by the "Law Reform in Transition States" project at the University of Bremen with the support of "Deutsche Gesellschaft für Technische Zusammenarbeit GmbH" (GTZ) at: <http://www.cis-legal-reform.org/civil-code/armenia/civ-arm-eng.htm>

Translator (with Alexei Zhiltsov) and editor, *The Civil Code of the Russian Federation*, with a Preface by A. Makovsky and an Introduction by A. Makovsky and S. Khokhlov (Armonk, N.Y.: M.E. Sharpe, 1997) (prepublished, without the Preface and Introduction in *Soviet Statutes and Decisions*, 1996-1997.

Translator (with Alexei Zhiltsov) and editor, *The Civil Code of the Russian Federation*, with a Preface by A. Makovsky and an Introduction by A. Makovsky and S. Khokhlov (Moscow: International Centre for Financial and Economic Development, 1997).

(With John Soma and James Sprowl), *1996 Supplement to Computer Law, Cases-Comments-Questions*, (St. Paul, Minn.: West Publishing Co., 1996).

The Mandelstam File, the Der Nister File: An Introduction to Stalin-Era Prison and Labor Camp Records (Armonk, N.Y.: M.E. Sharpe, 1996)

(With John Soma and James Sprowl), *Teacher's Manual for Use With Computer Law, Cases, Comments, and Questions*, (St. Paul, Minn.: West Publishing Co., 1992).

(With Glen E. Weston, and Roger Schechter), *Teacher's Manual for Use With Unfair Trade Practices and Consumer Protection, Cases and Comments, 5th ed.* (St. Paul, Minn.: West Publishing Co., 1992).

(With Glen E. Watson, and Roger Schechter), *Unfair Trade Practices and Consumer Protection, Cases and Comments*, 5th ed. (St. Paul, Minn.: West Publishing Co., 1992).

(With John Soma and James Sprowl), *Computer Law, Cases, Comments, and Questions*, (St. Paul, Minn.: West Publishing Co., 1992).

(Translator and co-editor with Robert Sharlet and Piers Beirne), *Stuchka: Selected Writings on Soviet Law and Marxism* (Armonk: M.E. Sharpe, 1988).

(With William E. Butler and John B. Quigley, Jr., co-editors), *Law After Revolution (New York: Oceana Publications*, 1988).

(With O.S. Ioffe), *The Soviet Economic System: A Legal Analysis* (Boulder: Westview, 1987).

(With James Sprowl), *Computer Applications in the Law* (St. Paul, Minn.: West Publishing Co.,

1987).

(With D.A. Loeber, editor-in-chief, Donald Barry, F.J.M. Feldbrugge, and George Ginsburgs, co-editors) *Ruling Communist Parties and Their Status Under Law* (Dordrecht: Martinus Nijhoff, 1986).

(With S. Chesterfield Oppenheim, Glen E. Weston, and Roger Schechter), *1986 Supplement to Unfair Trade Practices and Consumer Protection* (St. Paul, Minn.: West Publishing Co., 1986).

(With John N. Hazard and William E. Butler) *The Soviet Legal System: The Law in the 1980's (New York: Oceana Publications*, 1984).

(With S. Chesterfield Oppenheim, Glen E. Weston, and Roger Schechter) *Teacher's Manual for Use With Unfair Trade Practices and Consumer Protection, Cases and Comments, 4th ed.* (St. Paul, Minn.: West Publishing Co., 1983).

(With O.S. Ioffe) *Soviet Law in Theory and Practice* (New York: Oceana Publications, 1983).

(With S. Chesterfield Oppenheim, Glen E. Watson, and Roger Schechter) *Unfair Trade Practices and Consumer Protection, Cases and Comments*, 4th ed. (St. Paul, Minn.: West Publishing Co., 1983).

(With Gordon Smith and George Ginsburgs, co-editors) *Law and Economic Development in the Soviet Union* (Boulder, Colorado: Westview Press, 1982).

(With Gordon Smith and George Ginsburgs, co-editors) *Soviet and East European Law and the Scientific-Technical Revolution* (New York: Pergamon, 1981).

(With S. Chesterfield Oppenheim and Glen E. Weston) *1981 Supplement to Oppenheim and Weston's Unfair Trade Practices and Consumer Protection* (St. Paul, Minn.: West Publishing Co., 1981).

(Translator) *Pashukanis: Selected Writings on Marxism and Law*, edited by Piers Beirne and Robert Sharlet (London: Academic Press, 1979). Full text with original pagination available on the Internet at: <http://www.uiuc.edu/ph/www/p-maggs/pashukanis.htm>.

(With Donald Barry, F.J.M. Feldbrugge, and George Ginsburgs, co-editors) *Soviet Law After Stalin, III: Soviet Institutions and the Administration of Law* (Alphen aan den Rijn: Sijthoff & Noordhof, 1979).

(With Donald Barry and George Ginsburgs, co-editors) *Soviet Law After Stalin, II: Social Engineering through Law in the USSR* (Alphen aan den Rijn: Sijthoff & Noordhof, 1978).

(With Donald Barry and George Ginsburgs, co-editors) *Soviet Law After Stalin, I: The Citizen and the State in Contemporary Soviet Law* (Leiden: A.W. Sijthoff, 1977).

(With John N. Hazard & William E. Butler) *The Soviet Legal System*, 3d ed. (Dobbs Ferry, N.Y.: Oceana Publications, 1977).

(With John N. Hazard & Isaac Shapiro) *The Soviet Legal System*, 2nd ed. (Dobbs Ferry, N.Y.: Oceana Publications, 1969).

(With Harold J. Berman) *Disarmament Verification Under Soviet Law* (Dobbs Ferry, N.Y.: Oceana Publications, 1967).

Laws, Monographs, Translations, and Technical Reports

"Soviet Health Law" (400 pages of selected and translated legislative materials constituting Volume XX of Soviet Statutes and Decisions).

"Soviet Economic Law Reform" (400 pages of selected and translated legislative materials constituting Volume XIX of Soviet Statutes and Decisions).

"Soviet Higher Education Law" (400 pages of selected and translated legislative materials constituting Volume XVIII os Soviet Statutes and Decisions).

"Soviet Social Welfare Law" (400 pages of selected and translated legislative materials constituting Volume XVII of Soviet Statutes and Decisions).

"Soviet Labor Law" (800 pages of selected and translated legislative materials constituting Volumes XV and XVI of Soviet Statutes and Decisions).

"Soviet Copyright Law" (400 pages of selected and translated legislative materials and judicial decisions constituting Volume XIV of Soviet Statutes and Decisions).

"Soviet Patent Law" (400 pages of selected and translated legislative materials constituting Volume XIII of Soviet Statutes and Decisions).
Law and Population in Eastern Europe. Medford, Mass.: Fletcher School of Law and Diplomacy, Law and Population Monograph Series, No. 3 (1977).

Reporter (with Marion Benfield), Uniform Simplification of Land Transfers Act, Uniform Laws Annotated, Vol. 14, 209-349.

Reporter (with Marion Benfield, chief reporter), Uniform Land Transactions Act, 1975 Official Text with Comments, (St. Paul, Minn., West Publishing Co., 1976).

"Report of Research on Computer Model of the Legal Regulation of the Communist Economic Enterprise," American Philosophical Society Yearbook 1972 (Philadelphia, 1973), p. 496.

Representation of National and Regional Political Units in a Computerized World Future Model. Honolulu: East-West Population Institute, East-West Center, Worker Paper No. 27, October 1972.

Legal regulation of Population Movement to, from and within the United States--A Survey of Current Law and Constitutional Limitations. Honolulu: East-West Population Institute, East-West Center, Working Paper No. 25, June 1972.

Law and Population Growth in Eastern Europe. Medford, Mass.: Fletcher School of Law and Diplomacy, Law and Population Monograph Series, No. 3 [1972].

"A Proposal for Cooperation . . .," Second Symposium on the coordination of Research Concerning the Legal Systems of Central and Eastern Europe, Strasbourg, 1971. Document AS/Coll. RSJ (71) 17.

(With R.T. Chien and F.A. Stahl) New Directions in Legal Information Processing. Urbana, Ill.: University of Illinois Coordinated Science Laboratory, Report R-538, December 1971.

Nonmilitary Secrecy Under Soviet Law. RAND Corp. P-2856-1, 1964.

Articles

"The Uncertain Legal Status of Free and Open Source Software in the United States." In Axel Metzger ed., Free and Open Source Software (FOSS) and other Alternative License Models: A Comparative Analysis. *Ius Comparatum* – Global Studies in Comparative Law, Vol. 12, Springer International Publishing Switzerland, 2016, pp. 477-493.

"К вопросу о правовой охране ноу-хоу по российскому законодательству." [Regarding Legal Protection of Knowhow in Russian Legislation]. Труды по интеллектуальной собственности [Works on intellectual property]. Vol. XVII, No. 2, pp. 102-117. (2014).

"К вопросу о технических средствах защиты авторских и смежных прав." [Regarding Technical Measures of Protecting Copyright and Neighboring Rights] Труды по интеллектуальной собственности [Works on intellectual property] Vol. XVI, No. 1, pp. 102-115. (2014).

"License Contracts, Free Software and Creative Commons in the United States." American Journal of Comparative Law, Supplement, Volume 62 (Supplement) 2014, pp. 407-423.

"Lost in Translation (Interpretation)?" in *Liber Amicorum* in Honour of 50th Anniversary of Alexey Zhiltsov: Transational Trade and Law, compiled and edited by A. Muranov and V. Plekhanov, Moscow-Berlin, Infotropic Media, 2013, pp. 139-145.

"Islamic Banking in Kazakhstan Law," Review of Central and East European Law, Volume 36 (2011), pp. 1-32. http://www.law.illinois.edu/pmaggs/arts.htm.

"The Balance of Copyright in the United States of America," American Journal of Comparative Law, Supplement, Volume 58 (Supplement) 2010, pp. 369-376.

"Conflict of Laws in the Area of Intellectual Property" (in Russian) in a forthcoming Festschrift honoring M.M. Boguslavsky. (Corrected final proofs have been returned to publisher; awaiting publication).

"Unconscionability of the Arbitral Clause under United States Law," *Vestnik mezhdunarodnogo kommercheskogo arbitrazha*, Vol. I, No. 1 (2010), pp. 167-181.

"Reflections of Anglo-American Legal Concepts and Language in the New Russian Civil Code, " in William Simons, ed., *Private and Civil Law in the Russian Federation. Law in Eastern Europe: Essays in Honor of FJ.M. Feldbrugge,* 60 (Martinus Nijhoff: Leiden-Boston, 2009) 197-203.

"O prave na sekret proizvodstva (nou-khau). Kriticheskii analiz polozhenii IV chasti Grazhdanskogo kodeksa Rossiiskoi Federatsii" [The Right to Secrets of Production (Know-How). A Critical Analysis of Provisions of the Fourth Part of the Civil Code of the Russian Federation], *Voprosy pravovedeniia* (Questions of Legal Thought), 2009, No. 3-4, pp. 76-91.

"Zhong Ou ya guo jia min fa dian yi ge bi jiao xing de gai guan [On Eurasian civil codes], 74 *Graduate Law Review of CUPL* (2007), pp. 143-154.

"From Goldilocks to Micky Mouse - the Limits of Intellectual Property Protection," in Grazhdanskoe zakonodatel'stvo [Civil Legislation], Issue 27, edited by A.G. Didenko and E.A. Belianevich (Almaty, Kazakhstan, 2007), pp. 306-314. Also in Russian in the same volume as "Ot Zlatovlaski k Mikki Mausu - predely zashchity intellektual'noi sobstvennosti," pp. 294-305.

"Constitution of 1977," *Encyclopedia of Russian History.*

"High Arbitration Court," *Encyclopedia of Russian History*.

"Supreme Court," Encyclopedia of Russian History.

*"*Free Legal Advice on the Internet," *International Journal of Legal Information*, Vol. 34, No. 3 (Winter 2006), pp. 483-513.

"United States Courts Judge Transition Country Legal Systems," in Rechtslage von Auslandsinvestitionen in Transformationsstaaten (Berlin: Berliner Wissenschafts Verlag, 2006), pp. 529-539.

"Abusive Advertising on the Internet (SPAM) Under United States Law", 2006 *American Journal of Comparative Law, Supplement* 385-394, reprinted in John Kozyris, ed., *Regulating Internet Abuses: Invasion of Privacy* (Alphen aan den Rijn: Kluwer Law International, 2007), 203-211.

"Dietrich André Loeber," *Sudebnik,* Vol. 9 (2004), No. 2, p. 265.

"Public Land Ownership in the Russian Federation," in *Public Policy and Law in Russia: In Search of a Unified Legal and Political Space, Essays in Honor of Donald D. Barry, Law in Eastern Europe* 55, edited by Robert Sharlet and Ferdinand Feldbrugge (Leiden: Brill, 2005), pp. 199-211.

"Russia's Writing Requirement under the Convention on Contracts for International Sale of Goods," in *Balancing of Interests Liber Amicorum Professor Peter Hay zum 70. Geburtstag* (Frankfurt am Main: Verlag Recht und Wirtschaft GmbH, 2005), pp. 279-283.

"Commercial Law, 1917-1990s," in *Supplement to the Modern Encyclopedia of Russian, Soviet & Eurasian History*, Vol. 6, pp. 179-182.

"Civil Law in Russia, Soviet Union, Russian Federation," in *Supplement to the Modern Encyclopedia of Russia, Soviet & Eurasian History*, Vol. 6, pp. 117-123 (2005).

"Struggling towards Law? Human Rights and Legislative Reform in Moldova," in Ann Lewis, ed., *The EU and Moldova: On a Fault-line of Europe* (London: Federal Trust, 2004), pp. 149-154.

"Conflict of Laws and Russian-U.S. Intellectual Property Relations," in Alexander Trunck, Rolf Knieper, and Andrej G. Svetlanov, editors, Russland im Kontext der internationalen Entwicklung: Internationales Privatrecht, Kulturgüterschutz, geistiges Eigentum, Rechtsverinheitlichung; Russia in the International Context: Private International Law, Cultural Heritage, Intellectual Property, Harmonization of Laws; Rossiia v kontekste mezhdunarodnogo razvitiia: mezhdunarodnoe chastnoe pravo, zashchita kul'turnyskh tennostei, intellektual'naia sobststvennost', unifikatsiia prava: Festschrift für Mark Moiseevič Boguslavskij (Berlin: BMV Berliner Wissenschafts-Verlag, 2004).

"Judicial Precedent Emerges at the Supreme Court of the Russian Federation," 9 *The Journal of East European Law* 479-500 (2002). (actually published in 2004).

"Ronald Rotunda, Friend and Colleague," 2003 *University of Illinois Law Review* 1169-1170.

"The Effect of Proposed Amendments to Uniform Commercial Code Article 2," *University of Illinois Journal of Law, Technology and Policy*, 2002 U. Ill. J.L. Tech. & Pol'y 311.

"Soviet Law." *Encyclopaedia Britannica* 2003 http://www.britannica.com/eb/article?eu=70730 Also to appear in bound and CD-ROM editions.

"The '.us' Internet Domain," *American Journal of Comparative Law*, Vol. 50 Supplement (2002), pp. 297-318.

"*The Process of Codification in Russia:* Lessons Learned from the Uniform Commercial Code." *McGill Law Review*, Vol. 44, No. 2 (August 1999), 281-300.

"The Impact of the Internet on Legal Bibliography," *American Journal of Comparative Law*,

Vol. 46, Supplement 1998, pp. 665-675.

"Civil Law Reform and Privatization in the Newly Independent States," *Rule of Law Consortium Newsletter*, Spring 1998, pp. 3-4.

"Consumer Protection on the Internet," *Ajuris*, March 1998, pp. 105-112. (This is a paper presented at the First Interamerican Congress of Consumer Law.)

"The Russian Courts and the Russian Constitution," *Indiana International and Comparative Law Review*, Vol. 8, No. 1, pp. 99-117 (1997) (This is an expanded version of the Third John N. Hazard Lecture at the Association of the Bar of the City of New York.).

"The Mutual Restoration of Russian and United States Copyright," 3 *Parker School Journal of East European Law* 305-324 (1996).

"The Right Arbitration Forum Can Make the Difference Between Wining and Losing Disputes," *Russian Petroleum Investor*, June/July 1996, pp. 71-73.

"Russia's New Production Sharing Law Provides for Arbitration, But is Hampered by Politics," *Mealey's International Arbitration Report*, May 1996; reprinted in *Mealy's International Arbitration Review* 1996.

(With Robert Sharlet) "Reforming Legal Education in the Newly Independent States," *Rule of Law Consortium Newsletter*, Winter/Spring 1996, pp. 1-3.

"The Uniform Simplification of Land Transfers Act and the Politics and Economics of Law Reform," 20 *Nova Law Review* 1091- 1093 (1996).

"Industrial Property in the Russian Federation," in G. Ginsburgs et al., eds., *The Revival of Private Law in Central and Eastern Europe* (Leiden: Kluwer, 1996), pp. 377-90.

"The Russian Constitutional Court's Decisions on Residence Permits and Housing," 2 *Parker School Journal of East European Law* 561-582 (1995).

"Russian Commercial Courts Expand Jurisdiction Over International Business Disputes," *International Practitioner's Notebook*, August 1995, pp. 20-21.

"Legal Databanks in the United States and their Use in Comparative Law," 22 *International Journal of Legal Information*, 214-227 (1994).

"The Non-Role of Financial Intermediaries in Voucher Privatization in Russia, October 1992-February 1993," in Hans Smit & Vratislav Pechota, eds., *Privatization in Eastern Europe: Legal, Economic, and Social Aspects* (Irvington-on-Hudson: Transnational Juris Publications, 1994), 104-107.

"Overcoming Legal Obstacles to Doing Business in Russia," in *Law in Russia* (Donald W.

Treadgold Papers, No. 101, 1994), 18-27.

"Importing Russian Intellectual Property; the Interaction of Russian and United States Law," 1 *Parker School Journal of East European Law* (1994).

"The Use of Expert Systems in Comparative Law," United States national report prepared for the XIVth International Congress of Comparative Law, *American Journal of Comparative Law, Supplement 1994*, 801-812.

"International Trade and Commerce" in the proceedings of a conference on the work of Harold J. Berman, 42 *Emory Law Journal*, 449-473 (1993); reprinted in Harold O. Hunter, ed., *The Integrative Jurisprudence of Harold J. Berman* (Boulder: Westview Press, 1996), pp. 51-74.

"Russian International Arbitration Legislation, *International Arbitration Report*, Nov. 11, 1993, (Vol. 8, #11), pp. 16-18.

"The Role of Publishing Houses in Developing Legal Research and Publication," Académie intenationale de droit comparé- International Academy of Comparative Law, *Rapports Généraux XIIIe Congrè international Montreal 1990 XIIIth International Congress General Reports* (Cowansville, Québec: Yvon Blais, 1992), 961-967.

"Legal forms of doing business in Russia," *North Carolina Journal of International Law and Commercial Regulation*, Vol. 18, No. 1, pp 173-192 (1992).

With Leonid P. Malkov, "Protecting Intellectual Property in Russia," *Research-Technology Management*, Jan.-Feb. 1993 (Vol. 36, No. 1), pp. 15-16.

"New Russian Intellectual Property Legislation," *Mealey's Litigation Reports: Intellectual Property*, Dec. 28, 1992 (Vol. 1, #6), pp. 43-47.

"Substantive and Procedural Protection of Enterprise Rights," in Donald D. Barry, ed., *Toward the "Rule of Law" in Russia; Political and Legal Reform in the Transition Period* (Armonk, M.E. Sharpe, 1992), pp. 277-290.

Translator, "Soviet Enterprises on the Difficult Path to a Market Economy," by V.P. Mozolin, in Donald D. Barry, ed., *In Search of the Law Governed State: Political and Societal Reform Under Gorbachev* (1992).

"The Ministry of Finance," in Eugene Huskey, ed., *Executive Power and Soviet Politics; The Rise and Decline of the Soviet State*, (Armonk, M.E. Sharpe, 1992), pp. 129-142.

"Legal Rights of the Handicapped in the USSR," in *The Emancipation of Soviet Law* [*Law in Eastern Europe* No. 44], 1992, pp. 249-255.

"Developments in Arbitration Law in Russia, Ukraine, and Kazakhstan," *International Arbitration Report*, Nov. 1992, pp. 16- 18.

With Leonid P. Malkov, "Telfonye brokery." *Delovoi mir*, Sept. 18,1992, p. 15.

"Taking the 'Poison Pill': A Commentary on a Case Study," *Soviet Economy*, April-June 1992 (Vol. 8, No. 2), 158-163.

"Enforcing the Bill of Rights in the Twilight of the Soviet Union,"1991 *University of Illinois Law Review* 1049-1063.

"Legal Forms of Doing Business in Russia," 18 *North Carolina Journal of International Law and Com. Reg*. 173-192 (1992).

"Ownership Rights." In Michael P. Claudon and Tamar L. Gutner, *Investing in Reform: Doing Business in a Changing Soviet Union* (New York: New York University Press, 1991), pp. 155-169.

"Judicial Activism in the USSR." In Kenneth M. Holland, ed., *Judicial Activism in Comparative Perspective* (Houndmills: MacMillan, 1991), pp. 202-214.

"Post-Soviet Law: The Case of Intellectual Property Law." *Harriman Institute Forum*, Vol. 5, No. 3 (Nov. 1991), pp. 3-9.

"Special Section on the Fundamentals of Civil Law: Intellectual Property," *Soviet & East European Law*, 2 (1991), No. 6.

"Special Section on the Fundamentals of Civil Law: Choice of Law," *Soviet & East European Law*, 2(1991), No. 6.

"Law on Inventions," *Soviet & East European Law*, 2 (1991), No. 5.

"Systems for the Automated Storage and Retrieval of Legal Information: Their Use in Research on Foreign, Comparative, and International Law," *Proceedings of the XIIth International Congress of Comparative Law*.

"Recent Developments in Products Liability Law in the USA," *Journal of Consumer Policy* 14 (1991), 29-33.

"Product Liability Law in the US," *Australian Product Liability Reporter*, April 1991, pp. 7-9.

"Secret Soviet Economic Legislation," in *The Soviet Sobranie of Laws* (Berkeley: University of California, 1991), pp. 55-67.

"Edward Cleary as Colleague and Mentor," *University of Illinois Law Review*, 1990, 901-902.

"Marion Benfield as Colleague, Friend, Neighbor, Co-Reporter, and Fellow North Carolinian," *University of Illinois Law Review* (1990), 761-762.

(With co-authors Robert Sharlet et al., "P.I. Stuchka and Soviet Law," in *Revolution in Law, Contributions to the Development of Soviet Legal Theory*, 1917-1938 (Armonk: M.E. Sharpe, 1990), pp. 45-60.

"The 1987 Decree on The State Committee on Science and Technology," in Albert J. Schmidt, ed., *The Impact of Perestroika on Soviet Law* (Dordrecht: Martinus Nijhoff, 1990), pp. 289-298.

"Second Soviet Draft Law on Inventions Published," *Soviet & East European Law*, 1 (1990), 7, 10.
"Property and Rights of the Individual: Definition and Enforcement," *Moscow Conference on Law and Bilateral Relations* (1990), 169-171.

"U.S. and Soviet Barriers to Bilateral Trade: Using Trade as an Instrument of Foreign Policy, Currency Controls, Intellectual Property Protection, and the Authority to Contract," *Moscow Conference on Law and Bilateral Relations* (1990), 77-79.

"Facilitating U.S.-Soviet Joint Ventures Through Legislative Reform," *in Financial Markets, Joint Ventures, and Business Opportunities in the Soviet Union* (Middlebury: Geonomics Institute, 1990).

"Constitutional Implications of Changes in Property Rights in the USSR," *Cornell International Law Journal* 23 (1990) 363-375.

Participant in roundtable discussion, "Crises in the USSR: are the constitutional and legislative changes enough?" (Symposium: Perspectives on the Legal Perestroika; Soviet Constitutional and Legislative Changes), *Cornell International Law Journal* 23 (1990) 377-398.

"Access to Justice for the Consumer in the USA," *Journal of Consumer Policy*, 13 (1990), 45-58.

"The Restructuring of the Soviet Law of Inventions," *Columbia Journal of Transnational Law* 28 (1990) 277-289; reprinted in *Legal Reform in the USSR* (Transnational Juris Publications: Ardsley-on-Hudson, 1991).

(With co-author Ronald Rotunda), "Meanwhile, back in Mother Russia," *Legal Times*, Oct. 2, 1989, p. 35, col. 2.

"Systems for the Automated Storage and Retrieval of Legal Information: Their Use in Research on Foreign, Comparative, and International Law," *Proceedings of the XIIth International Congress of Comparative Law*.

"Administrative Law and Finance Law," in G. Ginsburgs, ed., *Soviet Administrative Law: Theory and Property* [*Law in Eastern Europe* No. 40] (Dordrecht: Martinus Nijhoff, 1989), 387-397.

"Reglament Arbitrazhnogo Instituta Stokgol'mskoi Torgovoi Palaty," *Arbitration International* 4

(1988) 331-333.

"The Role of Soviet Banking and Finance Law in Joint Enterprises," *Columbia Journal of International Business*, 23:2 (Summer 1988), 13-24.

"Introduction," in *Advertising Law Anthology*, Vol. XI (1988), ix- xii.

"Introduction," in *Model Jury Instructions for Business Tort Litigation*, 2nd ed. (Chicago: American Bar Association, 1988), xv-xxviii.

"Choice and Compulsion in Soviet Labor Law: Labor Conscription 1917-21," *Law After Revolution*, edited by William E. Butler, Peter B. Maggs, and John Quigley, Jr., (New York: Oceana Publications, 1988), 35-45.

"Law," a chapter of James Cracraft, ed., *The Soviet Union Today: an Interpretative Guide*, 2d ed. (Chicago: University of Chicago Press, 1987), pp. 339-348.

"Direct Contacts of Soviet Organizations in International Economic Relations," in *The Distinctiveness of Soviet Law* (Dordrecht: Martinus Nijhoff, 1987), pp. 183-195.

"Legal Regulation of the Dissemination of Scientific and Technical Information in the USSR," in Olimpiad S. Ioffe and Mark W. Janis, ed., *Soviet Law and Economy* (Dordrecht: Martinus Nijhoff, 1987), pp. 103-126.

"The League of Communists of Yugoslavia and the Law," in *Communist Parties and the Law*, (pp. 347-356).

"The Party of Labor of Albania and the Law," in Communist Parties and the Law, (pp. 211-221).

"Marxism and Soviet Environmental Law," *Columbia Journal of Transnational Law* 23 (1985) 510-522.

"Accounting," *Encyclopedia of Soviet Law*, 2nd ed. (Leiden, 1985), pp. 3-4.

"Budgets of Enterprises" *Encyclopedia of Soviet Law*, 2nd ed. (Leiden, 1985), pp. 92-93.

"Cooperatives," *Encyclopedia of Soviet Law*, 2nd ed. (Leiden, 1985), p. 184.

"Computers and the Law," *Encyclopedia of Soviet Law*, 2nd ed. (Leiden, 1985), p. 153.

"The Legal Impact of Modernization in the USSR," in *Law and Economic Development in the Soviet Union* (Boulder, Colorado: Westview Press, 1982), 1-10.

"Legal Aspects of the Computerization of Management Systems in the USSR and Eastern Europe," in *Law and Economic Development in the Soviet Union* (Boulder, Colorado: Westview Press, 1982), 133- 157.

"Computer Programs as the Object of Intellectual Property in the United States of America," *American Journal of Comparative Law*, 30 (1982), Supplement, 251-273.

"The Soviet Constitution . . ." *Human Rights*, 10 (1982), No. 2, pp. 34-39, 55-56.
"Land Records of the Uniform Simplification of Land Transfers Act," *Southern Illinois University Law Journal* (1981), 491-510.

"The Soviet Union's Approach to Coping with the Economic Aspects of National Security and Foreign Policy: The Soviet Legal Structure and the Development of Computer Technology," 1 *St. Louis University Public Law Forum*, 111-114 (1981).

"The Legal Structure of Technology Transfer in Eastern Europe," *Soviet and East European Law and the Scientific Technical Revolution*, edited by Gordon Smith, George Ginsburgs, and Peter B. Maggs (New York: Pergamon, 1981), 272-294.

"Socialist Law," *Academic American Encyclopedia*, Vol. 18, p. 25 (1981).

"New Life for Patents: Chakrabarty and Rohm and Haas Co.," *Supreme Court Review* (1980), 57-75.

"Characteristics of Soviet Tax and Budgetary Law," in Barry, Feldbrugge, Ginsburgs, and Maggs, eds., *Soviet Law After Stalin, III: Soviet Institutions and the Administration of Law*, (Alphen aan den Rijn: Sijthoff & Noordhoof, 1979), 93-106.

"Some Problems of Legal Protection of Programs for Microcomputer Control Systems," *University of Illinois Law Forum*, 1979, 453- 468.

"Automated Processing of Legal Information," *American Journal of Comparative Law*, Vol. 26 (Supplement) 1978: Law in the U.S.A. in the Bicentennial Era, 517-529.

"Improving the Legal Mechanisms for Economic Change," in Barry, Ginsburgs, and Maggs, eds., *Soviet Law After Stalin, II: Social Engineering Through Law* (Alphen aan den rijn: Sijthoff & Noordhoof, 1978), 117-138.

"Strict Law in Soviet Contract Law," in *The Unity of Strict Law: A Comparative Study*, ed. Ralph A. Newman. Brussels: Establissements Emile Bruylant, 1978, pp. 311-318.

"The Legal Status of Collective Farm Members," in *Soviet Law After Stalin, I: The Citizen and the State in Contemporary Soviet Law*. (Leiden: A.W. Sijthoff, 1977), 159-178.

"Remedies for Breach of Contract Under Article Two of the Uniform Land Transaction Act," *Georgia Law Review*, 11 (1977), 275-296.

"Teaching Law by Computer," *LeCourt*, 1 (1976), No. 2, pp. 10-13.

"Tube-watching in Law School," *Trial* 12 (1976), No. 12, pp. 32- 38.

(With Luke T. Lee), "North African Migrants Under Western European Law," *Texas International Law Journal*, 11 (1976), 225- 250; reprinted as *Law and Population Mongraph Series* No. 37 (1976) by the Law and Population Programme of the Fletcher School of Law and Diplomacy.

"Amnesty and Prisoner Population," *Soviet Union*, 3 (1976), 51-62.

"Legal Problems of Patents, Industrial Designs, Technical Data, Trademarks, and Copyrights in Soviet-American Trade," *Denver Journal of International Law and Policy*, 5 (1975), 311-322.

"Law and Sociology in Bulgaria: The Experiments with Pronatalist Legislation, *Review of Socialist Law*, 1 (1975), 253-260.

(With T.D. Mbody) "Computer-Based Legal Education at the University of Illinois: A Report of Two Years' Experience," *Journal of Legal Education*, 27 (1975), 138-156.

"Legal Controls on American Publication of Heterodox Soviet Writings," *Dissent in the USSR: Politics, Ideology, and People*, Ed. R.L. Tökés. Baltimore: John Hopkins, 1975, pp. 310-325.

"The Language of Codification: A Computer Analysis of the Family Code of the R.S.F.S.R.," *Codification in the Communist World*, Leiden: A.W. Sijthoff, 1975, pp. 239-290.

"Unification of Methods of Legal Automation," *Law in the United States in Social and Technical Revolution; Reports from the United States of America on Topics of Major Concern as Established for the IX Congress of the International Academy of Comparative Law*, Ed. J. Hazard & W.J. Wagner. Brussels: Establissements Emile Bruylant, 1974, pp. 677-694.

"A Computer Model of the System of Legal Regulation of the Soviet State Industrial Enterprise," *Contemporary Soviet Law: Essays in Honor of John N. Hazard*, ed. D.D. Barry, W.E. Butler & G. Ginsburgs. The Hague: Martinus Nijhoff, 1974, pp. 175-194.

"Compression of Legal Texts for More Economical Computer Storage, *Jurimetrics Journal*, 14 (1974). 254-261.

"New Directions in U.S.-U.S.S.R. Copyright Relations," *American Journal of International Law*, 68 (July 1974), 391-409.

"The Construction of a Concordance to the Uniform Commercial Code," *University of Illinois Law Forum*, 1974, 7-10.

(With W.D. Hawkland) "UCC Concordance,: *University of Illinois Law Forum*, 1974, 11-136; reprinted in William Hawkland, *Uniform Commercial Code Series*, Vol. 1, "Concordance Introduction," pp. 1-9, "Concordance," pp. 1-252.
"Accounting," *Encyclopedia of Soviet Law*, Ed. F. Feldbrugge. Leiden: A.W. Sijthoff, 1974, pp.

5-6.

"Budgets of Enterprises," *Encyclopedia of Soviet Law*, Ed. F. Feldbrugge. Leiden: A.W. Sijthoff, 1974, p. 90.

"Cooperatives," *Encyclopedia of Soviet Law*, Ed. F. Feldbrugge. Sijthoff, 1974, pp. 168-169.

"Englischsprachige Veröffentlichungen zum sowjetischen Zivil-und Wirtschaftsrecht," *Osteuropa-Recht*, 19 (1973), 283-299.

"Population Laws of Eastern Europe," Law and Population: *Lectures and Reading Materials Computer from the Seminar on Law and Population*, E.L. Lee. Medford, Mass.: Fletcher School of Law and Diplomacy, 1973, pp. 1-27.

"An Evolutionary Approach to Compatible Identifiers for Computerized Land Records," *Land Parcel Identifiers for Information Systems*, Ed. D. Moyer and K. Fisher. Chicago: American Bar Foundation, 1973, pp. 183-197.

"Automation of the Land Title System," *American University Law Review*, 22 (Winter 1973), 369-391, reprinted in R.N. Freed, *Computers and the Law—A Reference Work*. Boston: Freed, 4th ed. 1974, 467-478.

"A Computer Service Utility for the Legal Profession," *ACM Urban Symposium 1972*, Computers and Urban Society, pp. 133-146.

(With R.T. Chien and F.A. Stahl) "New Directions in Legal Information Processing," *1972 Spring Joint Computer Conference*, pp. 531-540.

(With Cary B. deBessonet) "Automated Logical Analysis of Systems of Legal Rules," *Jurimetrics Journal*, 12 (1972), 158-169.

"The Law of Farm-Farmer Relations," The Soviet Rural Community, ed. J.R. Millar. Urbana: University of Illinois, 1971, pp. 139- 156.

"Investment in Yugoslavia and Eastern Europe" (with co-author, Milan Smiljanic), *Journal of Law and Economic Development*, 4 (1969), 1-15.

"Negative Votes in Soviet Elections," Res Baltica, ed. A. Sprudz and A. Rusis. Leiden: Sijthoff, 1968, pp. 146-151.

"Unification of Law in Eastern Europe," *American Journal of Comparative Law*, 16 (1968), 107-126.
(With K. Winkler) "Libel in the Soviet Press: The New Civil Remedy in Theory and Practice," *Tulane Law Review*, 41 (December 1966), 55-74.

(With J.W. Jerz) "The Significance of Soviet Accession to the Paris Convention for the

Protection of Industrial Property," *Journal of the Patent Office Society*, 48 (April 1966), 242-263.

"Soviet Corporation Law: The New Statute on the Socialist State Production Enterprise," *American Journal of Comparative Law*, 14 (Summer 1965), 478-489.

"Les aspects juridiques de la planification economique en U.R.S.S.," *Annuaire de L'U.R.S.S.*, 3 (1965). 231-257.

"Der nichtmilitärische Geheimschutz nach Sowjetrecht," *Osteruropa Recht*, 11 (September 1965), 161-181.

"The Soviet Viewpoint on Nuclear Weapons in International Law," *Law and Contemporary Problems*, 29 (Autumn 1964), 956-970. Reprinted in *The Soviet Impact on International Law*, Ed. H.W. Baade. Dobbs Ferry, N.Y.: Oceana Publications, 1965.

"Commentary on 'Liberty, Law and the Legal Order,' " *Northwestern University Law Review*, 58 (November-December 1963), 657-662.

"The Security of Individually-Owned Property Under Soviet Law," *Duke Law Journal*, (Autumn 1961), pp. 525-537. Reprinted in Durham, N.C.: Duke University, World Rule of Law Center, *World Rule of Law Center Booklet Series*, No. 11.

Radio Talk

"Doing Business in Russia," *Common Ground Radio Series on World Affairs*, January 1994.

Educational Computer Programs

(Published on the PLATO/NOVANET Systems)

Contracts -- Offer and Acceptance

Contracts -- Statute of Frauds

(With Robert Platt) Regulated Industries -- Basic Legal Accounting

(With Thomas Mbody and Robert Platt) Regulated Industries -- Simulation Exercise

Legal Writing -- Citation Abbreviations
Legal Writing -- Latin Words and Phrases

Book Reviews

Review of Aleksei Gennad'evich Nazarov, *Predely osushchestvleniia iskliuchitelnogo prava na rezul'taty intellektual'noi deiatel'nosti* [Limits on the Exercise of the Exclusive Right to the

Results of Intellectual Activity], Review of Central and East European Law, 2015, No. 3-4, 375-376.

Review of William R. Spiegelberger, *The Enforcement of Arbitral Awards in Russia: Eleven Years of Commercial Court Practice Applying the New York Convention*, *Review of Central and East European Law*, Vol. 40, No. 2 (2015), pp. 203-204.

Review of *The Legal Dimension in Cold War Interactions: Some Notes from the Field*, ed. by Tatiana Borisova and William Simons, *Journal of Cold War Studies*, Vol. 16, No. 1, Winter 2014, pp. 244-245.

Review of Trygve Ben Holland, *Legal Commentary: Russian Competition Law* Trygve Ben Holland, Saarbrücker Verlag für Rechtswissenschaften, Saarbrücken, 2011, *Review of Central and East European Law*, 38 (2013) 195-196.

Review of *"The Judiciary in Central and Eastern Europe: Mechanical Jurisprudence in Transformation."* (*Law in Eastern Europe*, no. 61). By Zdenek Kühn. *Slavic Review*, 2012, p. 936.

Review of "*International Law: A Russian Introduction*. By V. I. Kuznetsov and B. R. Tuzmukamedov. Edited and translated by William E. Butler," to be published in *American Journal of International Law*, April 2010, p. 342.

Review of Patricia Kennedy Grimstead, F. J. Hoogewoud, and Eric Ketelaar, eds., *Returned from Russia: Nazi Archival Plunder in Western Europe and Recent Restitution.* Journal of Cold War Studies, Winter 2010, Vol. 12, No. 1, pp. 200-202.

Review of Noel Calhoun, *Dilemmas of Justice in Eastern Europe's Democratic Transitions*, Canadian American Slavic Studies, Vol. 41, No. 4, pp. 451-452 (2007).

Review of *Ruling Russia: Law, Crime, and Justice in a Changing Society*, ed. William Alex Pridemore, Slavic Review, Vol. 65, No. 3, pp. 614-615 (2006).

Review of W.E. Butler, *The Law of Treaties in Russia and the Commonwealth of Independent States: Text and Commentary.* Canadian American Slavic Studies, Vol. 38, No. 4, pp. 473-474 (2004).

Review of Soli Nysten-Haarala. *Russian Law in Transation: Law and Institutional Change,* Canadian American Slavic Studies, Vol. 37, No. 4, pp. 444-445 (2003).

Review of Hildegard Kochanek. *Die russisch--nationale Rechte von 1968 bis zum Ende der Sowjetunion: eine Diskursanalyse,* Canadian American Slavic Studies, Vol. 37, No. 4, pp. 443-444 (2003).

Abstract of Virginia Martin, *Law and Custom in the Steppe: The Kazakhs of the Middle Horde and Russian Colonialism in the Ninteenth Century*, Journal of the Central Eurasian Studies

Society, Vol. 2, No. 1 (Winter 2003), p. 26.

Review of Hiroshi Oda, *Russian Commercial Law*, American Journal of Comparative Law, Vol. 50, No. 4, pp. 875-877 (2002).

Review of Gordon Smith, *Reforming the Russian Legal System*, 61 Law and History Review 607-608 (1998).

Review of F.J.M. Feldbrugge, *Russian Law, the End of the Soviet System and the Role of Law*, 41 *American Journal of Comparative Law* 513-514 (1993).

Review of Antonio Boggiano, *International Standard Contracts: The Price of Fairness* (1991), *International Journal of Legal Information*, 20 (1992) 179-180.

Review of C. Prins, *Computer Program Protection in the USSR: A New Era for Socialist Copyright*, 1991. *Review of Central and East European Law*, 18 (1992) 293-296.

Review of Dencho Georgiev, *Suverenitetut v suvremennoto mezhdunarodno pravo I sutrudnichestvoto mezhdu durzhavite*, *American Journal of International Law*, 86 (1992), 438.

Review of Esa Paasivirta, *Participation of States in International Contracts and Arbitral Settlement of Disputes*, 1990. *International Journal of Legal Information*, 19 (1991) 260- 261.

Review of Heinz Schäffer and Attila Rácz, eds. (in collaboration with Barbara Rhode), *Quantitative Analyses of Law: A Comparative Empirical Study: Sources of Law in Eastern and Western Europe*, *International Journal of Legal Information*, 19 (1991) 136-137.

Review of Raymond Hutchings, *Soviet Secrecy and Non-Secrecy*, 1987. *The Russian Review*, 50 (1991) 379-380.

Review of Miodrag Sukijasovic, *Pravno regulisanje medunarodne trgovine kafom*, *American Journal of International Law*, 85 (1991) 249-50.

Review of William E. Butler, *Arbitration in the Soviet Union*, *International Journal of Legal Information*, 18 (1990), 169-170.

Review of Marc Maresceau, ed.*, The Political and Legal Framework of Trade Relations Between the European Community and Eastern Europe*, *International Journal of Legal Information*, 18 (1990), 90-91.

Review of *Medunarodno pravo mora i izvori medunarodnog prava*, *American Journal of International Law*, 84 (1990), 614-615.

Review of A.W. Koers, D. Kracht, M. Smith, J.M. Smits and M.C.M. Weusten, *Knowledge-Based Systems in Law: In Search of Methodologies and Tools* (1989). *International Journal of Legal Information* 17 (1989) 286-287.

Review of G.P.V. Vandenberghe, ed., *Advanced Topics of Law and Information Technology*, *International Journal of Legal Information* 17 (1989) 204.

Review of Arie Bloed, *The External Relations of the Council for Mutual Economic Assistance* and of George Ginsburgs, *The Soviet Union and International Cooperation in Legal Matters (Part 1): Recognition of Arbitral Agreements and Execution of Foreign Commercial Arbitral Awards*, *American Journal of International Law* 83 (1989) 701-702.

Review of O.N. Sadikov, *Soviet Civil Law* and of Olimpiad S. Ioffe, *Soviet Civil Law*. *Russian Review* 48 (1989) 227-228.

Review of Ernst-Joachim Mestm„ker (ed.), *The Law and Economics of Transborder Telecommunications*. *International Journal of Legal Information* 17 (1989) 104.

Review of P.D. Finn, *Essays on Contract*. *International Journal of Legal Information* 17 (1989) 55.

Review of H.W.K. Kaspersen, et al., *Telebanking, Teleshopping and the Law*. *International Journal of Legal Information* 68-69 (1989).

Review of Melville B. Nimmer and Paul Edward Geller (eds.*) International Copyright Law and Practice. International Journal of Legal Information* 17 (1989) 88.

Review of J.A. Keustermans and I.M. Arckens, *International Computer Law; A Practical Guide to the International Distribution and Protection of Software and Integrated Circuits*. *International Journal of Legal Information* 17 (1989) 82-84.

Review of Robert P. Bigelow, *Computer Contracts: Negotiating and Drafting Guide*. *International Journal of Legal Information*, 17 (1989) 189-190.

Review of Kazimierz Grzybowski, *Soviet International Law and the World Economic Order*. *Canadian-American Slavic Studies* (1989).

Review of E. Allan Farnsworth and Viktor P. Mozolin, *Contract Law in USSR and the United States: History and General Concept*. *Connecticut Journal of International Law*, 3 (1988) 519-523.

Review of Wolfgang Gößmann, *Die Kombinate in der DDR: Eine wirtschaftsrechtliche Untersuchung*. *Review of Socialist Law*, 14 (1988), 298-299.

Review of John N. Hazard, *Reflections of a Pioneering Sovietologist*. *International Journal of Legal Information* 16 (1988), 141.

Review of Daniel J. Meador, *Impressions of Law in East Germany; Legal Education and Legal Systems in the German Democratic Republic*. *University of Illinois Law Review* (1987), 543-545.

Review of Marie Helen Pichler, *Copyright Problems of Satellite and Cable Television in Europe*. *International Journal of Legal Information*, 16 (1988), 217-218.

Review of Stanley S. Arkin et al., *Prevention and Prosecution of Computer and High Technology Crime*. *International Journal of Legal Information*, 16 (1988), 237-238.

Review of M.M. Boguslavskii, *Mezhdunarodnoe ekonomicheskoe pravo*. *American Journal of International Law*, 81 (1987) 1007.

Review of John Livermore, *Exemption Clauses and Implied Obligations in Contracts. International* Journal of Legal Information, 15 (1987), 157-158.

Review of Henry Carr, *Computer Software: Legal Protection in the United Kingdom*. *International Journal of Legal Information*, 15 (1987) 181-182.

Review of Kojo Yelpaala, Maro Rubino-Sammartano, and Dennis Campbell, eds*., Drafting and Enforcing Contracts in Civil and Common Law Jurisdictions*. *International Journal of Legal Information*, 15 (1987), 76-77.

Review of *Yearbook on Socialist Legal Systems, 1986*. *American Journal of International Law*, 81 (1987), 821-822.

Review of Vojin Dmitrijevic, Strahovlada: *Ogled o ljudskim pravima I drzavnom teroru*. *American Journal of International Law*, 81 (1987), 799-800.

Review of Eugene Huskey, *Russian Lawyers and the Soviet State*. *American Historical Review*, 1987.
Review of Ger P. van den Berg, *The Soviet System of Justice: Figures and Policy*. *The Russian Review*, 1986.

Review of J. Fraser Mann; *Computer Technology and The Law in Canada*. *International Journal of Legal Information*, 15 (1987) 280-281.

Review of Bernard D. Reams, *University-Industry Research Partnerships*. International Journal of Legal Information, 14 (1986) 185-186.

Review of W.E. Butler and V.N. Kudriavtsev, eds., *Comparative Law and Legal System: Historical and Socio-Legal Perspectives*. *American Journal of International Law*, 80 (1986), 771-772.

Review of Danilo Türk, *Nacelo neintervencije v mednarodnih odnosih in v mednarodnem pravu*. *American Journal of International Law* 80 (1986), 403-404.

Review of James M. Swanson, *Scientific Discoveries and Soviet Law: A Sociohistorical analysis*. *American Historical Review*, (1986), 158-159.

Review of W.E. Butler, *Basic Documents on the Soviet Legal System*, 23 *American Journal of International Law*, 23 (1985), 521- 522.

Review of Hazard, *Managing Change in the USSR: The Politico- Legal Role of the Soviet Jurist* (1983). *International Journal of Legal Information*, 12 (1984), 162-163.

Review of Pretnar, *Inventor's Certificates, Rationalization Proposals and Discoveries* (1982). *American Journal of Comparative Law*, 32 (1984), 775-776.

Review of *The Soviet Union Through its Laws*, edited and translated by Leo Hecht. *Slavic Review*, 42 (1984), 320-3231.

Review of Ciampi, Femeli, and Trivisonno, *THES-BID: A Computer- Based Thesaurus of Terminology in Computers and the Law*. *International Journal of Legal Information*, 11 (1983), 90-91.

Review of Kourilsky, Racz and Schaffer, *The Sources of Law: A Comparative Empirical Study -- National Systems of Sources of Law*. *International Journal of Legal Information*, 11 (1983), 190-191.

Review of Rudolph and Strohbach: *Die rechtlich Regelung der internationalen Wirtschaftsbeziehungen der DDR zu Partnern im nichtsozialistischen Wirtschaftsgebiet*. *International Journal of Legal Information*, 11 (1983), 201-202.

Review of F.J.M. Feldbrugge, and William B. Simons, editors, *Perspectives on Soviet Law for the 1980s* (1982). *Soviet Union/Union Sovietique*, 10 (1983), 104.

Review of Konstantin Simis, *USSR: The Corrupt Society* and Logan Robinson, *An American in Leningrad*. *Slavic Review*, 42 (1983), 501-503.

Review of Milan Bulajic, *Medunarodno pravo ekonomskog razvoja: Pravni aspekti novog medunarodnog ekonomskog poretka*. *American Journal of International Law*, 77 (1983), 193.

Review of *The Soviet Codes of Law*, edited by William B. Simons. *Slavic Review*, 41 (1982), 729.

Review of Manfred Balz, *Eigentumsordmung und Technologiepolitik. Eine system-vergliechende Studie zum sowjetischen Patent-und Technologierecht*. *Review of Socialist Law*, 4 (1982), 392.

Review of *Deutsches und sowjetisches Wirtschaftsrecht; Rechtliche Aspekte der internen und bilateralen Wirtschaftsbeziehungen: Sowjetunion und BRD*. *Review of Socialist Law*, 4 (1982), 396.

Review of Mark Boguslavsky, *The USSR and International Copyright Protection*, translated by Yuri Shirokov. *Slavic Review*, 40 (1981), 122-123.

Review of Beith Krevitt Eres, *Legal and Legislative Information Processing*. *International Journal of Law Libraries*, 9 (1981), 119.

Review of Davorin Rudolf, *Neutralnost I paksaktivnost: Medunarodnopravni aspekti*. *American Journal of International Law*, 74 (1980), 490.

Review of Budislav Vukas, *Relativno djelovanje medunarodnih ugovora*. *American Journal of International Law*, 74 (1980), 248.

Review of George Dana Cameron III, *The Soviet Lawyer and His System: A Historical and Bibliographic Study*. *The Russian Review*, 39 (1980), 256.

Review of Serge L. Levitsky, *Copyright, Defamation, and Privacy in Soviet Civil Law*. The *Russian Review*, 39 (1980), 381-382.

Review of Gyula Eörsi, Comparative Civil (Private) Law; Law Types, Law Groups, the Roads of Legal Development. International Journal of Law Libraries, 8 (1980), 178-179.

Review of Benninger, *Die sowjetische Gesetzgebung zur rechtlichen Stellung des nichtehelichen Kindes unter besondere Berücksichtigung ihres Einflusses auf die Geburtenzhal*. *Review of Socialist Law*, Vol 4 (1978), 399-491.

Review of Michael A. Newcity, *Copyright Law in the Soviet Union*. *Russian Review*, 37 (1978), 472.

Review of Stanislaw J. Sawicki, *Soviet Land and Housing Law*. *Russian Review*, 37 (1978), 354-355.

Review of D.A. Loeber, *East-West Trade: A Sourcebook on the International Economic Regulations of Socialist Countries and Their Legal Aspects*. *American Journal of Comparative Law*, 25 (1977), 571-573.

Review of Manfred Balz, *Innovation and Invention Under Soviet Law. Technology and Culture*, 17 (1976), 561-562.

Review of Ronald A. May, ed. *Sense and Systems in Automated Law Research*. *American Bar Association Journal*, 62 (1976), 570-572.

Review of R.J. Erickson, *International Law and the Revolutionary State: A Case Study of the Soviet Union and International Law*. *American Political Science Review*, 70 (1976), 675-676.

Review of W. Kilian, *Juristiche Entscheidung und elektronische Datenverarbeitung*. *American Journal of Comparative Law*, 23 (1975) 772-773.

Review of J. Quigley, *The Soviet Foreign Trade Monopoly*. *American Journal of Comparative*

Law, 23 (1975), 154-156.

Review of E.W. Kitch and H.S. Perlman, *Legal Regulation of the Competitive Process, Cases, Materials and Notes on Unfair Business Practices, Trademarks, Copyright and Patents*. *Nebraska Law Review*, 52 (1973), 308-312.

Review of Gy. Eörsi and A. Harmathy, *Law and Economic Reform in Socialist Countries*. *American Journal of Comparative Law*, 21 (1973), 187-188.

Review of K. Grzybowski, *Soviet International Law, Doctrines and Diplomatic Practice*. *The Russian Review*, 31 (April 1972), 184- 185.

Review of J.N. Hazard, *Communists and Their Law*, and S. Kucherov, *The Bodies of Soviet Administration of Justice*. *Harvard Law Review*, 85 (December 1971), 530.

Review of S. Schwarz, *Sot'sial'noe strakhovanie v Rossii v 1917- 1919 godakh*. *American Historical Review*, 74 (June 1969), 1670.

Review of Conquest, *The Soviet Police System & Justice and the Legal System in the U.S.S.R. American Bar Association Journal*, 55 (January 1969), 168-169.
Review of M. Jaworskij, *Soviet Political Thought*. *American Journal of Comparative Law*, 16 (1968), 643.

Review of translations of Soviet Civil Legislation. *American Journal of Comparative Law*, 14 (1966), 729.

Review of Seara Vazquez, *Cosmic International Law*. *Journal of Legal Education*, 18 (1966), 490.

Review of J.F. Triska and R.M. Slusser, *The Theory, Law and Policy of Soviet Treaties*. *Slavic Review*, 22 (December 1963), 767.

Exhibit 2

Kaspersky-Branded Products and Berkeley Research Group Independent Assessment

NCCIC

Background

The Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) reviewed the Independent Assessment, titled *Information Security Risks of Anti-Virus Software* (hereafter "BRG Assessment"), prepared by Berkeley Research Group, LLC (BRG), and dated November 10, 2017. Kaspersky Lab (hereafter "Kaspersky") submitted the BRG Assessment to DHS as an exhibit to Kaspersky's request for DHS to initiate a review of Binding Operational Directive (BOD) 17-01. The BRG Assessment, in part, responds to the *NCCIC Information Security Risk Assessment* (hereafter "NCCIC Assessment") on commercial off-the-shelf (COTS) anti-virus software and Kaspersky-branded products, dated August 29, 2017. The NCCIC Assessment was attached as Exhibit 1 to an Information Memorandum from the Assistant Secretary for DHS Cybersecurity and Communications (CS&C) to the Acting Secretary of DHS, dated September 1, 2017 (hereafter "Information Memorandum"). This document is a *Supplemental Information Security Risk Assessment* and will similarly be attached to an Information Memorandum from the Assistant Secretary for CS&C to the Acting Secretary of DHS.

1. File Access and High-Level Privileges

The BRG Assessment confirms the key conclusions of the NCCIC Assessment. Specifically, 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." BRG describes the "kernel" as a "core component of a computer's operating system and largely responsible for facilitating the interaction between other software running on the computer and the computer's central processing unit (CPU), memory, and other hardware devices (often via additional software called a "device driver")."[1] The "SYSTEM account" is "an internal account on Microsoft Windows operating systems that operates at the highest privilege level."[2] Most anti-virus software now also "intercepts and monitors network traffic on a user's computer, including encrypted web browsing traffic, in order to identify malicious code embedded in websites visited by the user."[3]

Based on its "limited technical analysis within the time available" of Kaspersky and other anti-virus products, BRG determined that all of the software that it analyzed, including Kaspersky-branded products, "contained components that operated with SYSTEM-level privileges." Additionally, BRG determined that "[e]ach installed multiple kernel drivers within our test systems for various anti-malware purposes, including file system monitoring, process monitoring, and network traffic interception and

[1] BRG Assessment, p. 8, n. 13.

[2] BRG Assessment, p. 8, n. 14.

[3] BRG Assessment, pp. 8-9.

inspection."[4] BRG states that, "[A] software vulnerability in any one of the kernel drivers or SYSTEM-level processes could reasonably result in a complete compromise of the user's computer."[5]

While BRG refers (above) to a "software vulnerability" in a kernel driver or SYSTEM-level process, as detailed in the NCCIC Assessment, DHS is concerned about the information security risks presented by the normal functionality of anti-virus software, apart from any specific "vulnerability" in the software. The Russian Government or Kaspersky—in collaboration with the Russian Government—can exploit this functionality, including broad access to files, high-level system privileges, and interception and inspection of encrypted web traffic.

2. BRG Preliminary Review of Kaspersky-Lab Software

Overview

The BRG Assessment states that BRG conducted a "preliminary review" of specific Kaspersky anti-virus products and solutions. BRG states that the BRG Assessment intended the review to address the following three high-level objectives:

1. 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);
2. Determine whether turning KSN off—or using the Kaspersky Private Security Network (KPSN)—can reliability prevent potentially sensitive data from inadvertently being transmitted to Kaspersky; and
3. Evaluate whether there exists a mechanism by which a malicious actor leveraging KSN can conduct targeted searches of Kaspersky users for specific information.

NCCIC assesses each of these objectives in turn below.

Objective 1: Passive Interception and Decryption of Traffic between Kaspersky-Branded Products and KSN

Kaspersky's KSN infrastructure "supports several security-related services provided by Kaspersky software products, including file, website, and wireless network reputation services."[6] KSN also "has the ability to receive information from clients, such as statistics regarding malware detected on users' computers or samples of malicious files, to improve Kaspersky's malware detection capabilities."[7] These are all consistent with NCCIC's understanding of KSN functionality.

---

[4] BRG Assessment, p. 11.

[5] BRG Assessment, p. 11.

[6] BRG Assessment, p. 24.

[7] BRG Assessment, p. 24; see also p. 6, n. 6.

BRG indicates that it identified this objective because the NCCIC Assessment and the Information Memorandum "refer to KSN as a potential information security risk due to the presumed ability of a malicious third party to monitor and intercept communications between KSN and users of Kaspersky software."[8]

DHS notes two significant limitations in this portion of the BRG Assessment. First, as BRG states, "BRG has not yet independently reviewed any network protocols or other communications systems used *within* KSN or *between KSN and Kaspersky's non-KSN IT infrastructure* (e.g., Kaspersky offices or other datacenters)" (emphasis added by author).[9] It is this access to Kaspersky offices and datacenters in Russia—and communications between such offices and datacenters and KSN—that is a principal concern of DHS. In addition, BRG states that its objective is to evaluate the potential for "passive" monitoring and decryption by an intelligence agency or other third party. As explained in detail in the Information Memorandum, DHS is concerned—not only about such passive activities—but also about active operations involving Russian intelligence access to Kaspersky offices and datacenters, requests for decryption keys, and other abilities of Russian government agencies to compel or request assistance from Kaspersky.

On the specifics of what BRG did test, BRG states that it observed Kaspersky anti-virus software products "generally" using one of three network protocols for communicating with KSN infrastructure:

- Hypertext Transport Protocol (HTTP),
- HTTP Secure (HTTPS), and
- Kaspersky's proprietary KSN protocol.

Use of HTTP in Kaspersky Products

BRG states that Kaspersky client-side software uses HTTP to download product installation files during initial setup, to download software updates, and to download malware "record" updates. While other anti-virus vendors use the term "definition" or "signature," according to BRG, Kaspersky personnel internally use the term "record" to refer both to traditional signatures (used to identify malware on a user's computer) as well as more modern approaches to malware detection, such as heuristic methods, machine learning models, and behavioral methods.[10]

As BRG states, HTTP transmissions are unencrypted and unauthenticated. Nevertheless, BRG explains that all file types downloaded by Kaspersky software from Kaspersky servers are authenticated using "standard code- or package-signing mechanisms", including Microsoft's Authenticode and GOST 34.10.2001. Kaspersky software then "verifies the integrity of the bases or

[8] BRG Assessment, p. 24.

[9] BRG Assessment, p. 24, n. 71.

[10] BRG Assessment p. 8, n. 10.

index files prior to installation on the user's computer" and, consequently, users "would likely be able to detect attempts by a malicious actor to tamper with application-related files downloaded over HTTP."[11]

BRG does not explain exactly what error message would be presented to a user or any other mechanism by which a user would be alerted to a maliciously modified update. Moreover, BRG states that, "[d]ue to time constraints, we have not yet been able to include an assessment of Kaspersky's internal security processes and procedures regarding access to and use of [Kaspersky Lab Signer] and the keys used to sign bases, packages, or other updates distributed to Kaspersky software clients." [12] These are significant gaps in BRG's analysis. BRG's analysis of this use of HTTP therefore does not mollify DHS's concern that Kaspersky or Russian government actors could incorporate malicious functionality into Kaspersky software through the software or record update process.

Use of HTTPS in Kaspersky Products

BRG states that it observed Kaspersky software using HTTPS "in limited situations." Specifically, BRG explains that Kaspersky software will connect to KSN infrastructure:

- to activate the product;
- to obtain "in-product content" (such as Kaspersky Lab news);
- for communications about product license purchases and renewals; and
- for uploading "application crash dumps," which often include "the state of the application when the error occurred, possibly including memory contents, logs, or other information about the software on the system at the time of the application crash."[13]

BRG states that Kaspersky software "followed industry-standard best practices for SSL/TLS encryption," including using TLSv1.2 by default, properly validating the authenticity of server certificates, and using strong cipher suites for session key negotiation and encryption.[14]

DHS understands these uses of HTTPS and generally agrees with the use of HTTPS, if properly implemented, to protect web traffic. However, DHS notes that BRG states that it needs to "further validate the security of Kaspersky's client side SSL/TLS implementation (based on the open-source OpenSSL library), as well as the security processes used to manage the application servers."[15] Thus, if BRG identifies client-side implementation issues or issues with the security processes for management of Kaspersky application servers, these would present additional risks of concern to DHS.

---

[11] BRG Assessment, p. 25.

[12] BRG states that Kaspersky Lab Signer ("KLS") is Kaspersky's internal, centralized service "intended" to cryptographically sign the various file types used by Kaspersky software prior to distribution to users. BRG Assessment, p. 25.

[13] BRG Assessment, p. 25.

[14] BRG Assessment, p. 25.

[15] BRG Assessment, p. 26.

Breaking and Inspecting of HTTPS by Kaspersky Products

While BRG focuses on Kaspersky's use of HTTPS to encrypt communications between users and KSN, BRG does not address the risks created by the Kaspersky software's ability to break and inspect other HTTPS communications by the user's non-anti-virus applications.

As explained in the NCCIC Assessment, Kaspersky-branded products have the ability to decrypt encrypted HTTPS transmissions, inspect and analyze the contents, and then re-encrypt and forward on the traffic. Specifically, the NCCIC Assessment states, with respect to anti-virus products—including Kaspersky products that have this functionality—that the "antivirus software uses its own certificate to sign outgoing traffic from the user and incoming traffic from the server in order to decrypt the content and determine whether malicious commands or software are part of the communication. However, this technique expands the attack surface further, because it leaves no way for the client to independently validate its connection to the server."[16] Furthermore, "employing this function defeats the purpose of end-to-end encrypted HTTPS connections with an external server because a third party is allowed to read, manipulate, and forward any information in the connection."[17] And, "[i]n the worst case, a product could store and exfiltrate sensitive information, including login credentials being transmitted from the client to the server, or otherwise compromise the integrity of the network connection."[18]

Kaspersky's ability to break and inspect encrypted traffic is clearly described in publically-available Kaspersky documentation.[19] However, BRG's analysis does not address the above risks.

Use of Proprietary Encryption Protocol for Communications with the KSN

In addition to using HTTP and HTTPS, the BRG Assessment states that Kaspersky software uses "its own proprietary, encrypted protocol for communicating with KSN."[20] DHS understands that this custom protocol is the primary encryption method leveraged by Kaspersky products to protect sensitive customer information in-transit between the customer's Kaspersky software and KSN.

To analyze use of this protocol, BRG states that it reviewed a subset of the Kaspersky source code related to this protocol, communicated with a Kaspersky developer with knowledge of its implementation, and analyzed KSN network traffic generated by the Kaspersky products it was reviewing.[21] BRG then explains, at a high level, the various encryptions and decryptions—using certain public, private, and secret keys—that occur when Kaspersky client software first connects to KSN (e.g.,

---

[16] NCCIC Assessment, pp. 3-4.

[17] NCCIC Assessment, p. 4.

[18] NCCIC Assessment, p. 4.

[19] Kaspersky Lab, *How to scan encrypted connections in Kaspersky Internet Security 2012*, August 15, 2012, ID: 6271, https://support.kaspersky.com/us/6271.

[20] BRG Assessment, p. 26.

[21] *See* BRG Assessment, p. 26.

with a file reputation request), when the KSN server responds to the client software, and during future connections between the client and the KSN server.

BRG concludes that the KSN protocol "appears to be secure from decryption by a passive adversary who does not possess the server's RSA private key or secret [Advanced Encryption Standard] AES key ($\mathbf{K_s}$)." Significantly, the KSN protocol "does not provide forward secrecy"—i.e., "if the server's RSA private key [which is a long-term key shared across all KSN servers] is compromised, a malicious actor could decrypt the client-generated AES key ($\mathbf{K_c}$) and passively decrypt *all previous or subsequent data sent by or to a Kaspersky client*" (emphasis added by author).[22] Similarly, BRG states that "if the server's AES key [which is a secret key also shared across KSN servers and re-generated weekly] is compromised, a malicious actor could recover the client-generated AES key from the encrypted session token and use the decrypted AES key to passively decrypt *all previous or subsequent data sent by or to a Kaspersky client until the server rotates its AES key*" (emphasis added by author).[23]

BRG states that, according to Kaspersky, this proprietary, encrypted protocol is intended to "(a) reduce load on KSN clients and servers, (b) permit clients to continue an encrypted KSN session across multiple separate TCP connections, and (c) enable any KSN server to handle a client's request since the servers do not maintain any connection state."[24] However, as BRG explains, the encryption implementation creates significant risks to the confidentiality of the data transmitted between Kaspersky software and KSN servers, if a KSN RSA private key or an AES secret key is compromised or otherwise obtained. As DHS explains in the Information Memorandum to which this Supplemental NCCIC Assessment is attached, based on a report prepared by Professor Peter Maggs, Russian law requires Kaspersky—and all other companies that use encrypted communications—to provide to the Russian Federal Security Service (FSB) the keys or other information needed to decrypt the company's encrypted communications in Russia. Thus, DHS has significant concerns about the ability of FSB to obtain access to unencrypted transmissions between KSN and U.S. government customers that use Kaspersky-branded products and participate in KSN.

According to BRG, Kaspersky "has claimed that it is modifying its current KSN encryption protocol to incorporate a Diffie-Hellman key exchange protocol that would provide for forward secrecy."[25] The above issues nevertheless currently remain.

Objective 2: Turning KSN Off or Using the Kaspersky Private Security Network

As described in the NCCIC Assessment, DHS is aware of Kaspersky statements that user participation in KSN is voluntary and users can "disable telemetry [data] reporting completely at any given time."[26] However, BRG testing determined that this statement is inaccurate, at least with respect to Kaspersky

---

[22] BRG Assessment, pp. 26-27.

[23] BRG Assessment, pp. 26-27.

[24] BRG Assessment, p. 27.

[25] BRG Assessment, p. 27.

[26] NCCIC Assessment, p. 6.

consumer-oriented products; products which could be used by federal departments and agencies. Specifically, BRG observed that "Kaspersky consumer-oriented products (i.e., Kaspersky Anti-Virus, Kaspersky Internet Security, and Kaspersky Total Security), 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 by author).[27] In particular, when the software detected sample malware, BRG inferred that "statistics" about the infection were uploaded to Kaspersky— although BRG does not appear to know what exact data was uploaded—and that the sample file was "likely uploaded" to Kaspersky when KSN was enabled.[28] Thus, even if a customer declines to participate in KSN and disables KSN in the user interface, some data is transferred to Kaspersky, and even a sophisticated user is unable to determine exactly what that data is.

The NCCIC Assessment also acknowledged the ability of government customers to deploy a local version of KSN on the customer's network, referred to as the Kaspersky Private Security Network (KPSN). Kaspersky markets KPSN as a way for customers' files and other objects to be analyzed locally, in an IT environment controlled by the customer, rather than sending the files back to KSN over the public Internet (using the proprietary, custom protocol described above).

BRG explains that KPSN can be installed in one of three configurations: "(a) Standard, which allows all on-premise KPSN servers to access Kaspersky servers directly; (b) Unidirectional Gateway, in which access to Kaspersky servers is managed through a gateway, installed and configured in an organization's [demilitarized zone] DMZ, that allows only inbound traffic to the on-premise KPSN servers, and (c) Proxy, where traffic from the local network to the Internet is routed through a proxy server configured at the network's perimeter."[29]

In its testing, BRG observed its test KPSN server downloading and updating its reputational databases using HTTPS and AMQPS, an encrypted version of the Advanced Message Queuing Protocol. In response to a sample malware infection, a Kaspersky enterprise-oriented product (Kaspersky Endpoint Security) communicated (presumably about the detection) to the KPSN server, and BRG did not observe any traffic from the KPSN server to KSN or any other Kaspersky servers.[30]

However, BRG did not address a main concern expressed in the NCCIC Assessment about the KPSN option. Specifically, the NCCIC Assessment explains that

- "even on-premise solutions require vendor updates to the anti-virus signatures and less frequent updates to the software itself,"
- "these updates are usually downloaded via temporary or indirect Internet connection or physical media like USB flash drives," and

[27] BRG Assessment, p. 28.

[28] BRG Assessment, p. 28.

[29] BRG Assessment, p. 28.

[30] BRG Assessment, p. 29.

- "[a]ny software update has the potential to add functionality or expand the attack surface of the host machine."[31]

The Kaspersky client software still receives record and software updates from Kaspersky through KPSN, and such software updates can contain malware or take another action that presents risks to federal information and information systems (e.g., by compromising the integrity of data or the availability of IT resources; in addition to other mechanisms for data exfiltration outside of the connection between the customer and KSN).

The NCCIC Assessment also notes that a vendor-withheld signature would make the endpoint remain vulnerable to a known threat.[32] DHS recognizes that Kaspersky has pointed to NIST Special Publication 800-83, Revision 1 to argue that the risk of Kaspersky intentionally withholding signatures to allow specific attacks can be mitigated by using anti-virus products from multiple vendors. However, 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 that "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).[33] NIST also notes that this "would necessitate increased administration and training, as well as additional hardware and software costs."[34] Finally, this suggestion does not address the risks of software updates including malware, the risks of the increased attack surface and risk of vulnerabilities that come with deploying multiple anti-virus products, or other risks.

Objective 3: Risk of Leveraging KSN to Conduct Targeted Searches of Kaspersky Users for Specific Information

BRG explains that Kaspersky Lab Anti-Virus Architecture (KLAVA) is the architecture for the core component of the Kaspersky anti-virus products, the anti-virus "engine." According to BRG, the KLAVA anti-virus engine, like most anti-virus engines, operates by ingesting a set of algorithms defined by Kaspersky malware analysts to detect and, in some cases, remediate, a malware infection.[35] Kaspersky refers internally to the implementation of a particular detection algorithm as a record, which may contain the name or other identifier assigned to the threat, its signature, or other means of detecting the threat, and an action (the "verdict") to take if the software identifies a file or process matching the threat.[36] BRG explains that, in addition to signatures and more advanced detection methods, records may also

---

[31] NCCIC Assessment, p. 6.

[32] NCCIC Assessment, p. 6.

[33] NIST Special Publication 800-83, Rev. 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, July 2013, p. 11, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf.

[34] NIST Special Publication 800-83, Rev. 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, July 2013, p. 11, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf.

[35] BRG Assessment, p. 29.

[36] BRG Assessment, p. 29.

include references (called “links”) to executable procedures implemented in C/C++ code, and these links “have nearly unrestricted access to the user’s system, including the ability to call operating system [Application Programming Interfaces] or other low-level system functions.”[37] Additionally, records can be used to update and patch Kaspersky software.[38] Individual records are compiled and aggregated into multiple database files (called “bases”), which are stored in Kaspersky’s proprietary KDC file format and distributed for ingestion into the KLAVA engines.

Significantly, BRG explains that KLAVA provides a function “which allows the analyst to upload a file processed by KLAVA to Kaspersky for further analysis,” as well as additional functions that can be used to retrieve and upload other information, such as Microsoft Windows registry keys.[39] Depending on the record’s “verdict” section, Kaspersky may—or may not—notify the user about the detection.[40] Furthermore, because Kaspersky uses a proprietary file format and encryption, a customer is unable to access the records to analyze whether any might be malicious.

BRG concedes that it anticipates doing, but has not yet completed,

1. “a more comprehensive assessment of the circumstances in which a file will be uploaded to Kaspersky from a user’s computer”; and
2. “a review of Kaspersky’s operational processes related to any controls surrounding the development, testing, deployment, and auditability of records given their capabilities and breadth of system access.”[41]

BRG has not yet addresses either of these areas, both of which are of significant areas of concern for DHS.

3. Conclusion

The NCCIC Assessment explained various risks to federal information and information systems presented by Kaspersky-branded products. As detailed in this Supplement, the BRG Assessment confirms NCCIC’s concerns about the broad file access and high-level system privileges of Kaspersky anti-virus products and BRG’s “Preliminary Review” of Kaspersky anti-virus software, across three objectives, does not meaningfully address the information security risks identified by DHS.

[37] BRG Assessment, pp. 29-30.

[38] BRG Assessment, p. 29.

[39] BRG Assessment, p. 30.

[40] BRG Assessment, p. 30.

[41] BRG Assessment, p. 30.

Exhibit 3

NIST Special Publication 800-83
Revision 1

Guide to Malware Incident Prevention and Handling for Desktops and Laptops

Murugiah Souppaya
Karen Scarfone

http://dx.doi.org/10.6028/NIST.SP.800-83r1

COMPUTER SECURITY

National Institute of
Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-83
Revision 1

Guide to Malware Incident Prevention and Handling for Desktops and Laptops

Murugiah Souppaya
Computer Security Division
Information Technology Laboratory

Karen Scarfone
Scarfone Cybersecurity
Clifton, VA

http://dx.doi.org/10.6028/NIST.SP.800-83r1

July 2013

U.S. Department of Commerce
Cameron F. Kerry, Acting Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director

Authority

This publication has been developed by NIST to further its statutory responsibilities under the Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347. NIST is responsible for developing information security standards and guidelines, including minimum requirements for Federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate Federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), *Securing Agency Information Systems*, as analyzed in Circular A-130, Appendix IV: *Analysis of Key Sections*. Supplemental information is provided in Circular A-130, Appendix III, *Security of Federal Automated Information Resources*.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other Federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-83 Revision 1
Natl. Inst. Stand. Technol. Spec. Publ. 800-83r1, 47 pages (July 2013)
http://dx.doi.org/10.6028/NIST.SP.800-83r1
CODEN: NSPUE2

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in Federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

Malware, also known as malicious code, refers to a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system. Malware is the most common external threat to most hosts, causing widespread damage and disruption and necessitating extensive recovery efforts within most organizations. This publication provides recommendations for improving an organization's malware incident prevention measures. It also gives extensive recommendations for enhancing an organization's existing incident response capability so that it is better prepared to handle malware incidents, particularly widespread ones.

Keywords

incident response; information security; malware

Being able to alter application configuration settings quickly can be very beneficial in remediating vulnerabilities very quickly, including temporary remediation measures. For example, a configuration change could disable a vulnerable service temporarily while the service's vendor prepares and releases a patch that permanently fixes the vulnerability. Once the patch is available and deployed, the organization can reverse the configuration change to reactivate the no longer vulnerable service. Organizations should consider in advance how configuration settings could be changed in response to a malware emergency and establish and maintain appropriate procedures.

3.4 Threat Mitigation

Organizations should perform threat mitigation to detect and stop malware before it can affect its targets. Even if virtually all vulnerabilities in a host have been mitigated, threat mitigation is still critically important—for example, for stopping instances of malware that do not exploit vulnerabilities, such as attacks that rely on social engineering methods to trick users into running malicious files. Threat mitigation is also critical for situations where a major new threat is likely to attack an organization soon and the organization does not have an acceptable vulnerability mitigation option. For example, there might not be a patch available for a new vulnerability.

This section describes several types of security tools that can mitigate malware threats: antivirus software, intrusion prevention systems (IPS), firewalls, content filtering/inspection, and application whitelisting. For each of these categories, the section also describes typical features, the types of malware and attack vectors the tools address, and the methods they use to detect and stop malware. Recommendations and guidance for implementing, configuring, and maintaining the tools are also provided, as well as explanations of the tools' shortcomings and the ways in which they complement other tools. In addition, the section discusses client and server application settings that can be helpful in mitigating threats.

3.4.1 Antivirus Software

Antivirus software is the most commonly used technical control for malware threat mitigation. There are many brands of antivirus software, with most providing similar protection through the following recommended capabilities:

- Scanning critical host components such as startup files and boot records.
- Watching real-time activities on hosts to check for suspicious activity; a common example is scanning all email attachments for known malware as emails are sent and received. Antivirus software should be configured to perform real-time scans of each file as it is downloaded, opened, or executed, which is known as *on-access scanning*.
- Monitoring the behavior of common applications, such as email clients, web browsers, and instant messaging software. Antivirus software should monitor activity involving the applications most likely to be used to infect hosts or spread malware to other hosts.
- Scanning files for known malware. Antivirus software on hosts should be configured to scan all hard drives regularly to identify any file system infections and, optionally, depending on organization security needs, to scan removable media inserted into the host before allowing its use. Users should also be able to launch a scan manually as needed, which is known as *on-demand scanning*.
- Identifying common types of malware as well as attacker tools.

- *Disinfecting* files, which refers to removing malware from within a file, and *quarantining* files, which means that files containing malware are stored in isolation for future disinfection or examination. Disinfecting a file is generally preferable to quarantining it because the malware is removed and the original file restored; however, many infected files cannot be disinfected. Accordingly, antivirus software should be configured to attempt to disinfect infected files and to either quarantine or delete files that cannot be disinfected.

Organizations should use both host-based and network-based antivirus scanning. Organizations should deploy antivirus software on all hosts for which satisfactory antivirus software is available. Antivirus software should be installed as soon after OS installation as possible and then updated with the latest signatures and antivirus software patches (to eliminate any known vulnerabilities in the antivirus software itself). The antivirus software should then perform a complete scan of the host to identify any potential infections. To support the security of the host, the antivirus software should be configured and maintained properly so that it continues to be effective at detecting and stopping malware. Antivirus software is most effective when its signatures are fully up-to-date. Accordingly, antivirus software should be kept current with the latest signature and software updates to improve malware detection.

Organizations should use centrally managed antivirus software that is controlled and monitored regularly by antivirus administrators, who are also typically responsible for acquiring, testing, approving, and delivering antivirus signature and software updates throughout the organization. Users should not be able to disable or delete antivirus software from their hosts, nor should they be able to alter critical settings. Antivirus administrators should perform continuous monitoring to confirm that hosts are using current antivirus software and that the software is configured properly. Implementing all of these recommendations should strongly support an organization in having a strong and consistent antivirus deployment across the organization.

A possible measure for improving malware prevention is to use multiple antivirus products for key hosts, such as email servers. For example, one antivirus vendor might have a new signature available several hours before another vendor, or an organization might have an operational issue with a particular signature update. Another possibility is that an antivirus product itself might contain an exploitable vulnerability; having an alternative product available in such cases could provide protection until the issue with the primary product has been resolved. Because running multiple antivirus products on a single host simultaneously is likely to cause conflicts between the products, if multiple products are used concurrently, they should be installed on separate hosts. For example, one antivirus product could be used on perimeter email servers and another on internal email servers. This could provide more effective detection of new threats, but also would necessitate increased administration and training, as well as additional hardware and software costs.

Although antivirus software has become a necessity for malware incident prevention, it is not possible for antivirus software to stop all malware incidents. As discussed previously in this section, antivirus software does not excel at stopping previously unknown threats. Antivirus software products detect malware primarily by looking for certain characteristics of known instances of malware. This is highly effective for identifying known malware, but is not so effective at detecting the highly customized, tailored malware increasingly being used.

Exhibit 4

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

Homeland Security

September 1, 2017

INFORMATION

MEMORANDUM FOR THE ACTING SECRETARY

THROUGH: Chris Krebs
Senior Official Performing the Duties of the Under Secretary, NPPD

FROM: Jeanette Manfra
Assistant Secretary for Cybersecurity and Communications, NPPD

SUBJECT: **Proposed Binding Operational Directive 17-01, Removal of Kaspersky-Branded Products**

I. INTRODUCTION

This memorandum recommends that you issue a binding operational directive ("BOD") to all federal executive branch departments and agencies. You have statutory authority to issue BODs to safeguard federal information and information systems from known or reasonably suspected information security threats, vulnerabilities, and risks. BOD 17-01 would address information security risks presented by "Kaspersky-branded products." The term "Kaspersky-branded products" means information security products, solutions, and services supplied, directly or indirectly, by AO Kaspersky Labs, a Russian company, or any of its predecessors, successors, parents, subsidiaries, or affiliates (collectively, "Kaspersky").[1]

BOD 17-01 would require all federal executive branch departments and agencies to (1) identify the use or presence of Kaspersky-branded products on all federal information systems[2] within 30 days of BOD issuance; (2) develop and provide to DHS a detailed plan to remove and discontinue present and future use of all Kaspersky-branded products within 60 days of BOD

[1] BOD 17-01 does not apply to certain Kaspersky-branded services and Kaspersky code embedded in the products of other companies.

[2] For purposes of the BOD, "federal information system" means "an information system used or operated by an agency or by a contractor of an agency or by another organization on behalf of an agency." The BOD does not apply to statutorily defined "National Security Systems" nor to certain systems operated by the Department of Defense and the Intelligence Community. *See* 44 U.S.C. § 3553(d) & (e).

issuance; and (3) begin to implement the plan of action at 90 days after BOD issuance, unless directed otherwise by DHS in light of new information obtained by DHS or submitted by Kaspersky or any other entity that claims its commercial interests are directly impacted by the BOD.

DHS's cybersecurity experts in the National Protection and Programs Directorate, in consultation with interagency partners, agree that Kaspersky-branded products present known or reasonably suspected information security risks to federal information and information systems. This memorandum relies on an Information Security Risk Assessment (Exhibit 1) prepared by cybersecurity experts in the National Cybersecurity and Communications Integration Center ("NCCIC") within DHS,[3] as well as other public and non-public sources.

Currently, certain federal agencies use Kaspersky-branded products. Kaspersky also has plans to increase future sales of Kaspersky products to U.S. government customers.

BOD 17-01 is based on expert judgments about threats to U.S. national security. The danger stems in part from the inherent properties of anti-virus software, which operates with broad file access and elevated privileges. Such access and privileges can be exploited by a malicious cyber actor such as Russia, which has demonstrated the intent to target the U.S. government and the capability to exploit vulnerabilities in federal information systems. Kaspersky or the Russian government could use this software to engage in a wide range of malicious cyber activities against federal information and information systems, including exfiltrating files, modifying data, or installing malicious code, with potentially grave consequences for U.S. national security. These actions could take place because of a range of factors, including Russian laws that authorize the Russian Federal Security Service ("FSB") to compel Russian enterprises to assist the FSB in the execution of FSB duties, to second FSB agents to Russian enterprises (with the enterprise's consent), and to require Russian companies to include hardware or software needed by the FSB to engage in "operational/technical measures." Kaspersky also relies on the FSB for needed business licenses and certificates, and the FSB could condition the granting of such approvals on Kaspersky's cooperation. Finally, Russian law allows the FSB to intercept all communications transiting Russian telecommunication and Internet Service Provider networks, which presumably includes data transmissions between Kaspersky and its U.S. government customers. Because of these known or reasonably suspected risks to federal information and information systems, which directly implicate U.S. national security, this memorandum recommends that you exercise your authority to issue BOD 17-01.

After issuance of the BOD, Kaspersky will have an opportunity, through an administrative process that DHS is making available to Kaspersky and other entities whose commercial interests are directly impacted by the BOD, to submit additional information and arguments to DHS. The Department should remain open to hearing new information, review any such submission(s) closely, and adjust its analysis to the extent warranted.

This memorandum proceeds as follows. Part II provides a legal background on DHS's authority to issue BODs, and explains the rationale for issuing BOD 17-01 rather than pursuing debarment

[3] *See* 6 U.S.C. §§ 148; *see also* https://www.us-cert.gov.

of Kaspersky. Part III provides unclassified evidence in support of the BOD. Part IV references a classified annex that presents classified material relevant to the BOD. Part V analyzes the unclassified evidence in support of the BOD. Part VI analyzes available contrary evidence provided publicly by Kaspersky. Part VII concludes by recommending that you issue the BOD based on the unclassified record, and that classified material further supports this determination.

II. LEGAL BACKGROUND

A. Binding Operational Directive Authority

The Secretary of Homeland Security, in consultation with the Director of the Office of Management and Budget ("OMB"), administers the implementation of agency information security policies and practices for federal information systems, except for national security systems and certain systems of the Department of Defense and the Intelligence Community.[4] As part of that responsibility, the Secretary develops and oversees the implementation of BODs.[5]

A BOD is a compulsory direction to an agency that "(A) is for purposes of safeguarding Federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk; (B) shall be in accordance with policies, principles, standards, and guidelines issued by the Director [of OMB]; and (C) may be revised or repealed by the Director if the direction issued on behalf of the Director is not in accordance with policies and principles developed by the Director."[6] Agencies are required to comply with BODs.[7]

BODs are issued by DHS to implement federal information security policies, principles, standards, guidelines, and requirements, including "(A) requirements for reporting security incidents to the Federal information security incident center . . . ; (B) requirements for the contents of the annual [information security] reports . . . ; (C) requirements for the mitigation of exigent risks to information systems; and (D) other operational requirements as the Director or Secretary, in consultation with the Director, may determine necessary."[8]

DHS has developed BOD 17-01 in consultation with OMB, as well as other federal agencies, and OMB agrees with issuance of the BOD.

B. Debarment

The Federal Acquisition Regulation ("FAR") prescribes the policies and procedures governing the debarment and suspension of contractors by federal agencies.[9] In accordance with the FAR,

---

[4] 44 U.S.C § 3553(b), (e).
[5] *Id.* § 3553(b)(2).
[6] *Id.* § 3552(b)(1).
[7] *Id.* § 3554(a)(1)(B)(ii).
[8] *Id.* § 3553(b)(2).
[9] *See* FAR 9.400(a)(1). Note that the FAR only regulates suspension and debarment associated with U.S. government procurement. It does not regulate non-procurement spending. Non-procurement suspension and debarment rules are located in 2 CFR § 180.25.

suspension and debarment are discretionary administrative tools that are an appropriate means to exclude contractors that, for various reasons, have not been found to be responsible.[10]

A BOD under section 3553(b)(2) of title 44, U.S. Code is a more appropriate process than a debarment proceeding for addressing the information security risks posed by Kaspersky-branded products. First, a debarment would affect only future contracts for a finite period; it would not require federal agencies to remove products previously purchased and installed on federal networks, and thus would not address current information security risks to federal information systems. In fact the FAR allows agencies to continue contracts or subcontracts in existence at the time a contractor was debarred, suspended, or proposed for debarment. By contrast, the BOD addresses the removal and discontinuance of use of Kaspersky-branded products indefinitely (unless the BOD is terminated or modified by DHS). Second, debarment generally would not prohibit third parties (e.g., resellers) from selling products produced by a debarred party; instead, debarment only prohibits the debarred company itself from contracting with the U.S. government.

III. UNCLASSIFIED EVIDENCE RELEVANT TO BOD 17-01

This Part presents unclassified evidence relevant to BOD-17-01. In particular, this Part includes evidence showing that Kaspersky-branded products are present on federal information systems; that those products could be exploited by a malicious actor to cause various significant effects on agency information and information systems; that Russia is a malicious cyber actor that has targeted the U.S. government; that Kaspersky has ties with the Russian government, and therefore may assist in achieving Russian objectives; and that, even without active Kaspersky assistance, Russian government agencies have authorities and access to data that could be leveraged by virtue of Kaspersky's operations being headquartered in Russia. Finally, similar concerns have been recognized by a range of credible government officials and agencies, including the heads of five U.S. intelligence agencies and the General Services Administration.

Further analysis of this evidence is presented in Part V below, followed by a summary of contrary evidence and an analysis thereof in Part VI below.

A. Kaspersky-branded products currently are, and absent agency action will likely continue to be, used in U.S. government information systems.

According to a DHS analysis of network traffic between federal agencies and known Kaspersky domains, as well as follow-up engagement with specific agencies, it is clear that a number of federal agencies use Kaspersky software as part of their anti-virus solution.

Moreover, Kaspersky has expressed its intention to expand its business with U.S. government customers. According to a 2015 press release announcing the appointment of a General Manager for Kaspersky Government Security Solutions, Inc. ("KGSS"), a wholly owned subsidiary of Kaspersky Lab North America, the General Manager "will be responsible for developing the strategic business vision for KGSS and exploring tactical partnerships that will provide the

[10] *See* FAR 9.402(a).

organization's unique cybersecurity services and solutions to U.S. government, U.S. government contractors and the U.S. National Critical Infrastructure sector."[11]

B. Anti-virus software, including Kaspersky-branded products, present a range of information security risks.

1. All Kaspersky-branded products within the scope of BOD 17-01 contain anti-virus functionality or are services that present other information security risks.

Based on a review of Kaspersky's website, all of the following software products or solutions named in BOD 17-01 are or contain anti-virus software: Kaspersky Anti-Virus; Kaspersky Internet Security; Kaspersky Total Security; Kaspersky Small Office Security; Kaspersky Endpoint Security Cloud; Kaspersky Endpoint Security for Business Select; Kaspersky Endpoint Security for Business Advanced; Anti Targeted Attack, Endpoint Security; and Cloud Security. 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 entity.

In addition to products and solutions that contain anti-virus functionality, the BOD applies to all cybersecurity services supplied, directly or indirectly, by Kaspersky, including Threat Hunting, Incident Response, and Security Assessment,[12] with the exception of two Kaspersky services explicitly excluded from the scope of the BOD: Kaspersky Threat Intelligence and Kaspersky Security Training. The information security risks presented by the services covered by the BOD are addressed in the NCCIC Assessment discussed below.

2. Anti-virus software has broad access to files, operates with elevated privileges, and has other capabilities that could be exploited by a malicious cyber actor.

DHS cybersecurity experts at NCCIC have prepared an Information Security Risk Assessment (the "NCCIC Assessment") regarding both commercial anti-virus software generally and Kaspersky-branded products specifically.[13] With respect to anti-virus software generally, the NCCIC Assessment explains the three signature detection methods used by anti-virus software (file scanning, heuristics, and general decryption), and further explains that "antivirus software requires the highest level of system privileges" to perform its functions, including "full content inspection capabilities." This level of system privileges creates various information security risks, including the ability to remove and transmit files or data back to company servers; to "break" encrypted (HTTPS) web traffic, permitting the interception of otherwise encrypted communications; and to manipulate updates to the anti-virus software's "definitions" (i.e., a list of "signatures" against which files on the device are compared) to intentionally not identify malicious files as malicious.

---

[11] Exhibit 2 (Kaspersky Press Release, *KGSS Appoints Cynthia James as General Manager*, 7 January 2016, https://usa.kaspersky.com/about/press-releases/2016_kgss-appoints-cynthia-james-as-general-manager).

[12] *See* Exhibit 3 (Kaspersky website, *Cybersecurity Services*, https://usa.kaspersky.com/enterprise-security/cybersecurity-services).

[13] Exhibit 1 (NCCIC Information Security Risk Assessment: COTS Antivirus Software and Kaspersky-Branded Products, as of 29 August 2017).

The NCCIC Assessment is supported by similar statements by other cybersecurity experts. Matthew Green, an assistant professor and cryptography researcher at Johns Hopkins' Information Security Institute, quoted in the publication *DefenseOne*, stated: "Anti-virus is really powerful[.] . . . It has to be powerful to do what it does. It explores every nook and cranny of a computer and you can't restrict it. It can change the way an operating system works. It can bypass a lot of features of the operating system. It has almost total visibility into every [email] attachment."[14] Based on "security researcher" sources, *DefenseOne* concluded: "At its most basic level, anti-virus does its work by regularly scanning every single file and system on a computer. Because it does this on the computer itself rather than at the periphery of an entire network, there usually aren't other systems monitoring the work of the anti-virus. . . . When the anti-virus finds something suspicious in a file, it will quarantine that file for additional, automated investigation. . . . If the anti-virus sees something that looks suspicious but isn't a known infection—say, for instance, a file that may be infected with polymorphic malware constantly changing its particular digital signature—it may encrypt that file and transport it to the AV company's own systems for investigation."[15] Regarding the risks posed by anti-virus software, the article states: "It could install something malicious on a computer that poses as a security update, security researchers say. Even easier, it could decline to install certain updates that protect against preferred attack vectors of a particular adversary. It would also be relatively easy to skip certain updates for only a subset of customers, security researchers say. Or, simplest of all, the anti-virus could simply extract files an adversary might find interesting under the premise those files were being scanned for infections."[16]

3. Kaspersky-branded products present the traditional risks of anti-virus software, plus additional risks if customers participate in the Kaspersky Security Network.

With respect to Kaspersky-branded products, the NCCIC Assessment states: "Based on publicly available information, Kaspersky-branded antivirus software and other Kaspersky-branded products and solutions that contain antivirus functionality appears to present the general antivirus software risks" identified regarding anti-virus software generally. This includes the potential for a malicious actor to exploit the software to exfiltrate files, modify system behavior, and install malicious code through software updates.

In addition, the NCCIC Assessment explains that additional information security risks are raised if a customer participates in the Kaspersky Security Network ("KSN"). For example, under the terms of the KSN Statement to which participating users must agree, Kaspersky users agree to the transfer of "highly sensitive data collected from a user's device, such as information about any files downloaded, web sites visited, running applications, user account names, software installed on the computer, and essentially the full spectrum of forensic data a device produces."

---

[14] Exhibit 4 (Joseph Marks, *The US Government is Still Installing Russian Software on its PCs*, Defense One, 15 June 2017, http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/?oref=d-channeltop).

[15] Exhibit 4 (Joseph Marks, *The US Government is Still Installing Russian Software on its PCs*, Defense One, 15 June 2017, http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/?oref=d-channeltop).

[16] Exhibit 4 (Joseph Marks, *The US Government is Still Installing Russian Software on its PCs*, Defense One, 15 June 2017, http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/?oref=d-channeltop).

NCCIC assesses that this data could be used to launch additional cyber intrusions into customer devices.

In an interview with MSNBC, Eugene Kaspersky confirmed that Kaspersky anti-virus software scans "all the data" on the computers on which it is installed, "like any other anti-virus product."[17] Moreover, Kaspersky customers must agree to a KSN Statement to participate in the KSN. The KSN Statement for Kaspersky Endpoint Security for Windows 10, by way of example, includes an extensive list (more than 5 pages, single spaced) of the information that the user agrees to "automatically provide" as part of participation in the KSN, including "whole files or parts of files" that, in Kaspersky's determination, "could be exploited by intruders to harm the User's computer."[18]

Finally, the cybersecurity services supplied by Kaspersky and covered by BOD 17-01 present various information security risks, even if the services do not involve installation of anti-virus software. As recognized by NCCIC, "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."

C. Russia is a significant cybersecurity threat to U.S. government information and information systems.

In a statement to the Senate Intelligence Committee regarding the most recent Worldwide Threat Assessment of the U.S. Intelligence Community, the Director of National Intelligence assessed: Russia is a "full-scope cyber actor that will remain a major threat" to the U.S. government, among other targets; Russia has a "highly advanced offensive cyber program, and in recent years, the Kremlin has assumed a more aggressive cyber posture"; and "Russian cyber operations will continue to target the United States and its allies to gather intelligence . . . and prepare the cyber environment for future contingencies."[19]

Russian cyber-attacks pose a challenge to global security: the Norwegian and Dutch governments assert that Russian attacks illustrate the severity of the Russian cyber-threat to both the United States and its allies.[20] In a hearing on the 2015 Worldwide Threat Assessment of the U.S. Intelligence Community, the Director of National Intelligence testified before the Senate Armed Services Committee that "the Russian cyber threat is more severe than we had previously

---

[17] Exhibit 5 (The Rachel Maddow Show, *Russian Kaspersky Lab faces new scrutiny, suspicion*, On assignment with Richard Engel, 28 July 2017, at 8:55-9:12, http://www.msnbc.com/rachel-maddow/watch/russian-kaspersky-labs-faces-new-scrutiny-suspicion-1012640835507).

[18] Exhibit 6 (Kaspersky Security Network Statement for Kaspersky Endpoint Security 10 for Windows, Section B, http://support.kaspersky.com/9365#block0).

[19] Exhibit 7 (Daniel R. Coats, Statement for the Record to the Senate Select Committee on Intelligence, *Worldwide Threat Assessment of the US Intelligence Community*, p. 1, https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf).

[20] Exhibit 8 (Statement of Janis Sarts, *Russian Intervention in European Elections: Hearing Before the Senate Select Committee on Intelligence*, 115th Cong., 3, 28 June 2017, https://www.intelligence.senate.gov/sites/default/files/documents/sfr-jsarts-062817b.pdf).

assessed,"[21] and his Statement for the Record states: "Cyber threats to US national and economic security are increasing in frequency, scale, sophistication, and severity of impact."[22] These reports are confirmed by private sector security companies.[23] This threat represents the "new normal" as the Intelligence Community assesses that Russian intelligence services will continue to "develop capabilities to provide Putin with options to use against the United States."[24]

Publicly-available sources further indicate that Russia has specifically targeted U.S, government information and information systems. For example, then-Secretary of Defense Ashton Carter revealed publicly that Russian hackers had breached a Department of Defense unclassified computer network.[25]

In a Joint Analysis Report and other analytic products, DHS and the Federal Bureau of Investigation ("FBI") also detailed the tools and infrastructure used by Russian civilian and military intelligence services to compromise and exploit networks and endpoints associated with the U.S. elections in 2016 (malicious cyber activity collectively referred to as "GRIZZLY STEPPE").[26] On December 28, 2016, President Obama issued Executive Order 13757, which sanctioned, among other parties, the FSB and the GRU in connection with Russian malicious cyber activities to undermine the 2016 Presidential election.[27]

These reports illustrate that Russia is a significant cybersecurity threat to the U.S. government, and Russia has become increasingly aggressive in its cyber operations in recent years. Therefore, Russia likely would leverage any available access into U.S. government information systems, including through Kaspersky-branded products.

---

[21] Exhibit 9 (Franz-Stefan Gady, *Russia Tops China as Principal Cyber Threat to US*, The Diplomat, 3 March 2015, http://thediplomat.com/2015/03/russia-tops-china-as-principal-cyber-threat-to-us/).

[22] Exhibit 10 (James Clapper, Statement for the Record to the Senate Armed Services Committee, *Worldwide Threat Assessment of the US Intelligence Community*, p. 5, 26 February 2015, https://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf).

[23] *See* Exhibit 11 (Cory Bennett, *Russia's cyberattacks grow more brazen*, The Hill, 12 April 2015, http://thehill.com/policy/cybersecurity/238518-russias-cyberattacks-grow-more-brazen) ("Crowdstrike has recorded over 10,000 Russian intrusions at companies worldwide in 2015 alone. That's a meteoric rise from the 'dozens per month' that [CEO Dmitri] Alperovitch said the firm noted this time last year, just as the U.S. was imposing its sanctions.").

[24] Exhibit 12 (Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent US Elections*, Intelligence Community Assessment, p. 15, 6 January 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf) (noting that "[i]mmediately after Election Day, we assess Russian intelligence began a spearphishing campaign targeting US Government employees[,] think tanks, and NGOs, and "[t]his campaign could provide material for future influence efforts as well as foreign intelligence collection on the incoming administration's goals and plans").

[25] Exhibit 13 (Fox News, *Carter reveals Russians hacked Pentagon's network*, 24 April 2015, http://www.foxnews.com/politics/2015/04/23/carter-reveals-russians-hacked-pentagon-network.html).

[26] Exhibit 14 (DHS and FBI Joint Analysis Report (JAR) 16-20296A, *GRIZZLY STEPPE—Russian Malicious Cyber Activity*, 29 December 2016, https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf), as updated and expanded by Exhibit 15 (DHS Analysis Report (AR) 17-20045, *Enhanced Analysis of GRIZZLY STEPPE Activity*, 10 February 2017, https://www.us-cert.gov/sites/default/files/publications/AR-17-20045_Enhanced_Analysis_of_GRIZZLY_STEPPE_Activity.pdf).

[27] Exhibit 16 (Office of Foreign Assets Control, *Issuance of Amended Executive Order 13694; Cyber-Related Sanctions Designations*, dated 29 December 2016 but linking to 28 December 2016 Executive Order, https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20161229.aspx).

D. Kaspersky has ties to the Russian intelligence and other government agencies.

1. Kaspersky may have developed products with the FSB and at least one Kaspersky product is approved to handle Russian state secrets.

The Federal Security Service ("FSB") is a Russian intelligence agency. It also has a regulatory role in licensing companies to engage in encryption-related activities and handle state secrets, as well as issuing certificates for individual products that use encryption and/or process state secrets.[28] While Kaspersky obtains licenses and certificates from the FSB like other regulated companies, Kaspersky has obtained certificates and licenses that suggest an unusually close relationship between Kaspersky and the FSB.

According to an article by McClatchy's Washington Bureau, "several" of Kaspersky's certificates dating to 2007 include a "military intelligence unit number matching that of an FSB program," which a "former Western intelligence official" who examined the documents for McClatchy described as "very unusual" and which the article states is "[u]nlike the stamped approvals the FSB routinely issues to companies seeking to operate in Russia."[29] The article includes a picture of one such certificate, which shows the number "43753."[30] Similarly, a study by Taia Global from 2012 includes an image of a certificate from 2011 that also includes number "43753," with an explanatory box stating "VCH 43753 is CBS FSB." The study states earlier that "CBS FSB" is the FSB Communications Security Center and "Vch" 43753 refers to a "Military Unit."[31]

The DHS Office of Cybersecurity and Communications ("CS&C") reviewed the images of the certificates, and a translation of the certificates indicates that they were issued by the FSB Communications Security Center. Moreover, a translation of the 2007 certificate in the McClatchy article shows that the certificate was issued "to military unit 43753 closed joint stock company [JSC] Kaspersky Lab." Similarly, the 2011 certificate shown in the Taia Global study was issued to "closed JSC Kaspersky Lab, military unit 43753." In both cases, this language in

---

[28] *See* Exhibit 17 (Taia Global Inc., *Russian Laws and Regulations: Implications for Kaspersky Labs*, posted at this *Wired* URL: https://www.wired.com/images_blogs/dangerroom/2012/07/Russian-Laws-and-Regulations-and-Implications-for-Kaspersky-Labs.pdf); *see also* Exhibit 18 (Federal Law on the Federal Security Service of the Russian Federation, Articles 12.j, 13.x, unofficial translation, dated 24 February 2012 and current through Federal Law No. 424-FZ of 8 December 2011, prepared by the Council of Europe, http://www.icla.up.ac.za/images/un/use-of-force/eastern-europe/Russia/Federal%20Law%20on%20Federal%20Security%20Service%20Russia%201995.pdf).

[29] Exhibit 19 (David Goldstein and Greg Gordon, *Documents could link Russian cybersecurity firm Kaspersky to FSB spy agency*, McClatchy Washington Bureau, 3 July 2017, http://www.chicagotribune.com/news/nationworld/ct-kaspersky-cyber-russia-spy-agency-20170703-story.html).

[30] Exhibit 19 (David Goldstein and Greg Gordon, *Documents could link Russian cybersecurity firm Kaspersky to FSB spy agency*, McClatchy Washington Bureau, 3 July 2017, http://www.chicagotribune.com/news/nationworld/ct-kaspersky-cyber-russia-spy-agency-20170703-story.html).

[31] Exhibit 17 (Taia Global Inc., *Russian Laws and Regulations: Implications for Kaspersky Labs*, posted at this *Wired* URL: https://www.wired.com/images_blogs/dangerroom/2012/07/Russian-Laws-and-Regulations-and-Implications-for-Kaspersky-Labs.pdf). The Taia Global study references both 437535 and 43753. It appears that the "437535" inadvertently includes an extra "5" at the end.

the certificates suggests that Kaspersky Lab either *is* military unit 43753 or *is part* of military unit 43753.

In addition, according to a *Bloomberg* article, based on internal emails from Kaspersky (which are not posted with the article), in 2009 Mr. 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 that's deployed around the world to corporations (but, noticeably, is not available in the U.S. or Canada)."[32] The article notes that Kaspersky instructs senior staff to keep the project secret, according to internal company emails that the company admits are authentic.[33]

Finally, according to a 2012 study by Taia Global, Kaspersky was, at that time, one of only two anti-virus companies licensed by the FSB to work with Russian government state secret information.[34] More recently, Kaspersky products have been approved to handle Russian state secrets. For example, in November 2016, Kaspersky obtained a certificate for Kaspersky Anti-Virus 8 for Mac, which certified that the anti-virus software "complies with the requirements of the FSB of Russia for antivirus products" of classes B2, V2, and G2, which can be used for the protection of information/data containing "information [or data/intelligence] constituting a state secret."[35] Kaspersky's approval to handle state secrets indicates at least that it is trusted by the FSB.

1. *Kaspersky officials have ties to Russian intelligence, the Ministry of Defense, and other Russian government agencies.*

Eugene Kaspersky, co-founder of Kaspersky, has various personal and professional ties to Russian government agencies. He graduated in 1987 from the Institute of Cryptography, Telecommunications and Computer Science, which was sponsored by the KGB (the predecessor to the FSB), the Ministry of Defense, the Soviet Space Agency, and the Ministry of Atomic Energy.[36] After graduating, he worked for the Ministry of Defense.[37] More recently, according

---

[32] Exhibit 20 (Jordan Robertson, *A Russian Cybersecurity Company's Ties to the Kremlin*, Bloomberg Technology, 11 July 2017, https://www.bloomberg.com/news/articles/2017-07-11/a-russian-cybersecurity-company-s-ties-to-the-kremlin).

[33] Exhibit 20 (Jordan Robertson, *A Russian Cybersecurity Company's Ties to the Kremlin*, Bloomberg Technology, 11 July 2017, https://www.bloomberg.com/news/articles/2017-07-11/a-russian-cybersecurity-company-s-ties-to-the-kremlin).

[34] Exhibit 17 (Taia Global Inc., *Russian Laws and Regulations: Implications for Kaspersky Labs*, posted at this *Wired* URL: https://www.wired.com/images_blogs/dangerroom/2012/07/Russian-Laws-and-Regulations-and-Implications-for-Kaspersky-Labs.pdf).

[35] Exhibit 21 (Excerpt of Kaspersky Certificates webpage, as archived by WayBackMachine on 28 June 2017, https://web.archive.org/web/20170628062336/http://www.kaspersky.ru/about/why/certificates/certificates-government).

[36] Exhibit 22 (Eugene Kaspersky, *A practical guide to making up a sensation*, Nota Bene: Official Blog of Eugene Kaspersky, 20 March 2015, https://eugene.kaspersky.com/2015/03/20/a-practical-guide-to-making-up-a-sensation/).

[37] Exhibit 22 (Eugene Kaspersky, *A practical guide to making up a sensation*, Nota Bene: Official Blog of Eugene Kaspersky, 20 March 2015, https://eugene.kaspersky.com/2015/03/20/a-practical-guide-to-making-up-a-sensation/). *Wired* and MSNBC have indicated that Mr. Kaspersky was involved in intelligence activities, but Mr. Kaspersky stated that he was a software engineer. *See* Exhibit 23 (Noah Shachtman, *Russia's Top Cyber Sleuth Foils US Spies, Helps Kremlin Pals*, Wired, 23 July 2012, https://www.wired.com/2012/07/ff_kaspersky/all/); Exhibit 5 (The Rachel Maddow Show, Russian Kaspersky Lab faces new scrutiny, suspicion, On assignment with Richard Engel, 28 July

to a *Bloomberg Business* article from 2015, "[u]nless [Mr.] Kaspersky is travelling, he rarely misses a weekly *banya* (sauna) night with a group of about 5 to 10 that usually includes Russian intelligence officials."[38]

According to *Bloomberg*, Chief Legal Officer Igor Chkunov is a "former KGB officer."[39] He "regularly joins Mr. Kaspersky's banya nights" and "is the point man for the company's work with the Russian government, three of the insiders say. Since 2013, he has managed a team of 10 specialists who study data from customers who have been hacked and provide technical support to the FSB and other Russian agencies. The team can access data directly from any of the company's systems. While Kaspersky Lab's managing director for North America, Christopher Doggett, says its data are anonymous, two people familiar with the technology say it can be altered to gather identifying information from individual computers and has been used to aid the FSB in investigations."[40]

Kaspersky's Chief Operating Officer, Andrey Tikhonov, started his career in information technology in 1989 at a "research institute of the Russian Ministry of Defense, rising to the rank of lieutenant-colonel" and, earlier, graduated from a "military academy in Kiev."[41]

According to a *Bloomberg* article from 2015, Kaspersky's ties to the Russian government "dramatically increased after two waves of executive departures," according to four former Kaspersky "insiders." The first came in 2012, after Kaspersky ended an IPO partnership with Greenwich, Connecticut investment firm General Atlantic. Afterward, according to the article, Kaspersky's Chief Business Officer Garry Kondakov "circulated an internal email saying that from then on, the company's highest positions would be held only by Russians, say two people who saw the e-mail. Board meetings, once conducted in English, were now in Russian.[42] Kaspersky has stated that it searched its archives and did not find the email.[43]

2017, 10:15-10:25, http://www.msnbc.com/rachel-maddow/watch/russian-kaspersky-labs-faces-new-scrutiny-suspicion-1012640835507); Exhibit 22 (Eugene Kaspersky, *A practical guide to making up a sensation*, Nota Bene: Official Blog of Eugene Kaspersky, 20 March 2015, https://eugene.kaspersky.com/2015/03/20/a-practical-guide-to-making-up-a-sensation/).

[38] Exhibit 24 (Carol Matlack, Michael Riley, Jordan Robertson, *The Company Securing Your Internet Has Close Ties to Russian Spies*, Bloomberg Businessweek, 19 March 2015, updated 20 March 2015, https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies).

[39] Exhibit 25 (Jordan Robertson and Michael Riley, *Kaspersky Lab Has Been Working With Russian Intelligence*, Bloomberg Businessweek, 11 July 2017, https://www.bloomberg.com/news/articles/2017-07-11/kaspersky-lab-has-been-working-with-russian-intelligence).

[40] Exhibit 24 (Carol Matlack, Michael Riley, Jordan Robertson, *The Company Securing Your Internet Has Close Ties to Russian Spies*, Bloomberg Businessweek, 19 March 2015, updated 20 March 2015, https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies).

[41] Exhibit 26 (Biography of Andre Tikhonov on Kaspersky website, https://usa.kaspersky.com/about/team/andrey-tikhonov).

[42] Exhibit 24 (Carol Matlack, Michael Riley, Jordan Robertson, *The Company Securing Your Internet Has Close Ties to Russian Spies*, Bloomberg Businessweek, 19 March 2015, updated 20 March 2015, https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies).

[43] Exhibit 22 (Eugene Kaspersky, *A practical guide to making up a sensation*, Nota Bene: Official Blog of Eugene Kaspersky, 20 March 2015, https://eugene.kaspersky.com/2015/03/20/a-practical-guide-to-making-up-a-sensation/).

E. Russian law and other factors may facilitate FSB exploitation of Kaspersky software.

1. The FSB has authorities to compel or request assistance from Russian companies.

According to a 2012 report by Taia Global, an unofficial translation of the Federal Law on the Federal Security Service (the FSB) of the Russian Federation (No. 40-FZ) provided by the Council of Europe, and a review of the current law by CS&C, the FSB has a wide range of intelligence authorities, including engaging in foreign intelligence activities, using undercover agents, and using special methods and means to carry out intelligence and counter-intelligence activities.[44] Moreover, Russian enterprises (among other parties) are obligated to assist the FSB "in the execution of the duties assigned to" the FSB. In addition, providers of "electronic communications services of all types" are obligated, at the FSB's request (and without a requirement for the enterprise's consent), "to include in the apparatus [also translated as devices/systems] additional hardware and software and create other conditions required" by the FSB "to implement operational/technical measures." Furthermore, for the purpose of "safeguarding the security of the Russian Federation," FSB "servicemen" may be seconded to Russian enterprises, with the enterprise's consent and in accordance with procedures established by Russia's President, while the servicemen remain on military service.[45] As stated by the Taia Global report from 2012: "If the FSB asks for your help, you help. If they ask you to modify hardware or software . . . so they can execute an operation or monitor a network, you do it. And if they want to place someone i[n] your organization to support FSB objectives, they can do so with your management[']s permission."[46]

Similarly, according to another Russian law (Federal Law No. 144-FZ on Operational-Search Activities), the FSB and other bodies are granted the right to "engage in operational-search activity in Russia." "Operational-search activity" includes collecting information "creating a threat to the military, economic or ecological security" of Russia and taking information off "technical communication channels" and other means of communication; individual persons "may be drawn, with their consent, into the preparation or the carrying out of the operational-search measures"; such persons are "obliged to keep in secret the information, which they have

---

[44] Exhibit 18 (Federal Law on the Federal Security Service of the Russian Federation, Articles 13.a.1, c.1, and t, unofficial translation, dated 24 February 2012 and current through Federal Law No. 424-FZ of 8 December 2011, prepared by the Council of Europe, http://www.icla.up.ac.za/images/un/use-of-force/eastern-europe/Russia/Federal%20Law%20on%20Federal%20Security%20Service%20Russia%201995.pdf).

[45] Exhibit 27 (Current version of Federal Law No. FZ-40, in Russian, accessed on 21 August 2017); Exhibit 17 (Taia Global Inc., *Russian Laws and Regulations: Implications for Kaspersky Labs*, posted at this *Wired* URL: https://www.wired.com/images_blogs/dangerroom/2012/07/Russian-Laws-and-Regulations-and-Implications-for-Kaspersky-Labs.pdf); Exhibit 18 (Federal Law on the Federal Security Service of the Russian Federation, Articles 13, 15, unofficial translation, dated 24 February 2012 and current through Federal Law No. 424-FZ of 8 December 2011, prepared by the Council of Europe, http://www.icla.up.ac.za/images/un/use-of-force/eastern-europe/Russia/Federal%20Law%20on%20Federal%20Security%20Service%20Russia%201995.pdf); *see also* Exhibit 28 (Brief of *Amici Curiae* Privacy International and Human Rights Watch, *In the Matter of the Search and Seizure of an Apply iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203*, p. 13, 3 March 2016, https://www.privacyinternational.org/sites/default/files/Amicus%20Brief%20-%20PI%20and%20HRW.pdf).

[46] Exhibit 17 (Taia Global Inc., *Russian Laws and Regulations: Implications for Kaspersky Labs*, posted at this *Wired* URL: https://www.wired.com/images_blogs/dangerroom/2012/07/Russian-Laws-and-Regulations-and-Implications-for-Kaspersky-Labs.pdf).

obtained in the course of the preparation or of the carrying out of the operational-search measures"; all information collected, as well as sources, methods, results, and other information, are classified as state secrets; and neither citizenship nor place of domicile can be an obstacle to collecting the information.[47]

2. *SORM and/or conditions on government approvals may permit or facilitate FSB access to Kaspersky customer data.*

According to an analysis by the Library of Congress, a decision of the European Court of Human Rights, and other sources, the FSB is able to remotely monitor all data and voice communications transiting the networks of Russian telecommunications companies and internet service providers pursuant to a court order that does not need to be provided to the provider, or without a court order if there is an imminent threat that a crime may be committed, under a system collectively referred to as "SORM" (translated in certain sources as "System for Operative-Investigative Measures" or "System for Ensuring Investigative Activities").[48] Any transmission of Kaspersky customer data through Russian networks would be subject to this authority. Even if such transmissions were encrypted, Russian government agencies may have leverage (e.g., as a condition to issuing licenses and certificates needed by Kaspersky) to request or require that Kaspersky or Russian telecommunications providers provide keys to decrypt encrypted data transmissions or otherwise provide access to customer data.

---

[47] Exhibit 29 (Current version of Federal Law No. 144-FZ, in Russian, accessed on 21 August 2017); Exhibit 30 (Federal Law No. 144-FZ of August 12, 1995 on Operational-Search Activities, as amended through 24 July 2007, Articles 1, 2, 6, 8, 12, 17, https://www.wto.org/english/thewto_e/acc_e/rus_e/WTACCRUS58_LEG_373.pdf).

[48] *See, e.g.*, Exhibit 31 (Library of Congress, *ECHR, Russian Federation: Breaches of Human Rights in Surveillance Legislation*, Global Legal Monitor, 2 March 2016, http://www.loc.gov/law/foreign-news/article/echr-russian-federation-breaches-of-human-rights-in-surveillance-legislation/) ("Russian SORM legislation consists of a set of regulations issued over the years by the Federal Council of Ministers and the Ministry of Communications and Information Technologies requiring telecommunications service providers to purchase and maintain communications interception equipment on their own as a requirement to stay in business and to conclude a nondisclosure agreement with the Federal Security Service (FSB) guaranteeing access by intelligence and other special services to communications conducted over the operated network"); Exhibit 32 (Andrei Soldatov and Irina Borogan, *Russia's Surveillance State*, World Policy Journal, Fall 2013, http://www.worldpolicy.org/journal/fall2013/Russia-surveillance) ("The FSB has control centers connected directly to operators' computer servers. To monitor particular phone conversations or Internet communications, an FSB agent only has to enter a command into the control center located in the local FSB headquarters. This system is replicated across the country. In every Russian town, there are protected underground cables, which connect the local FSB bureau with all Internet Service Providers (ISPs) and telecom providers in the region."); Exhibit 33 (James A. Lewis, *Reference Note on Russian Communications Surveillance*, CSIS, 18 April 2014, https://www.csis.org/analysis/reference-note-russian-communications-surveillance) ("Collection requires a court order, but these are secret and not shown to the service provider."); Exhibit 34 (Baker and McKenzie, *Doing Business in Russia 2017*, § 23.7, http://www.bakermckenzie.com/-/media/files/insight/publications/doing-business-in/bk_russia_doingbusiness_2017.pdf?la=en) ("SORM provides the opportunity to control communications without the participation of the provider. According to the law, such investigations are allowed only under a court order, or if there is an imminent threat that a crime maybe committed."); Exhibit 35 (Freedom House, *Freedom on the Net 2016*, Russia, p. 684, November 2016, https://freedomhouse.org/sites/default/files/FOTN_2016_Full_Report.pdf) ("The current version, SORM-3, uses DPI [i.e., deep packet inspection] technology, enhancing the ability of the security services to monitor content on all telecommunications networks in Russia.").

3. Russia has other levers of influence over Kaspersky and its employees.

According to experts, the Russian government has other levers of influence over people and companies operating in Russia. Michael Morrell, the former Deputy Director of the CIA, recently told CBS News: "There is a connection between Kaspersky and Russian intelligence, and I'm absolutely certain that Russian intelligence would want to use that connection to their advantage."[49] McClatchy quotes Steve Hall, a "former CIA station chief in Moscow" who "later headed the agency's Russian operations before retiring in 2015." According to the article, Hall stated: "These guys' families, their well-being, everything they have is in Russia[.] . . . Any time (Russian President Vladimir Putin) wants Kaspersky to do something – anything – he'll remind them that's where their families are and where their bank accounts are. There's no doubt in my mind it could be, if it's not already, under the control of Putin." Similarly, according to a former FBI Executive Assistant Director, regardless of whether Mr. Kaspersky wants to run his business independently or not cooperate, if a Russian intelligence service sought access to information held by Kaspersky, "you don't have a choice" and "regardless of whether Eugene Kaspersky would even want to do it or not, when it comes down to the way they run their government, there's no choice involved there."[50]

4. Activities of Russian security services may differ from publicly-available legal provisions.

As stated by the Council of Europe's Venice Commission, "security agencies tend to be governed by 'unpublished rules and by classified policy decisions, which would not and could not be brought to the attention of the public or of the Commission. Deficient legal provisions might well have been corrected in practice or, vice-versa, good legal provisions might not be applied in the intended way in practice.'"[51]

F. Other government officials have expressed concern with Kaspersky products.

At a Senate Intelligence Committee hearing in May 2017, Senator Rubio asked the following to Daniel Coats, Director of National Intelligence; Michael Pompeo, Director, CIA; Andrew McCabe, Acting Director, FBI; Admiral Michael Rogers (USN), Director, NSA; Robert Cardillo, Director, NGA; and Lt. Gen. Vincent Stewart (USMC), Director, DIA: "[W]ould any of you be comfortable with the Kaspersky Lab software on your computers?" In response,

---

[49] Exhibit 36 (CBS News, *W.H. cybersecurity coordinator warns against using Kaspersky Lab software*, 22 August 2017, https://www.cbsnews.com/news/kasperksy-lab-software-suspected-ties-russian-intelligence-rob-joyce/).

[50] Exhibit 5 (The Rachel Maddow Show, *Russian Kaspersky Lab faces new scrutiny, suspicion*, On assignment with Richard Engel, 28 July 2017, 16:03-16:20, http://www.msnbc.com/rachel-maddow/watch/russian-kaspersky-labs-faces-new-scrutiny-suspicion-1012640835507).

[51] Exhibit 37 (European Commission for Democracy Through Law (Venice Commission), *Opinion on the Federal Law on the Federal Security Service (FSB) of the Russian Federation*, CDL-AD(2012)015, adopted by the Venice Commission At its 91st Plenary Session (Venice, 15-16 June 2012), ¶ 7, http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2012)015-e) (quoting CDL-AD(2007)016).

McCabe said, "A resounding no, from me." Pompeo: "No." Coats: "No, Senator." Rogers: "No, sir." Stewart: "No, Senator." Cardillo: "No, sir."[52]

In addition, the Chairman of the House Committee on Science, Space, and Technology has expressed serious concerns about the company's products. On July 27, 2017, Rep. Lamar Smith, the Committee's Chairman, sent a letter to various federal agencies. The Committee's press release states: "Compromised anti-virus has the potential to undermine the security and integrity of any system on which it is installed, and could do so without detection[.]" 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."[53]

Furthermore, on July 11, 2017, the General Services Administration ("GSA") removed Kaspersky-manufactured products from the GSA IT Schedule 70 and GSA Schedule 67 (Photographic Equipment and Related Supplies and Services) because "GSA's priorities are to ensure the integrity and security of U.S. government systems and network and evaluate products and services available on our contracts using supply chain risk management processes."[54] NASA also removed Kaspersky products from its Solutions for Enterprise-Wide Procurement (SEWP) contract vehicle.[55]

Finally, on July 18, 2017, the California Department of General Services ("DGS"), in partnership with the California Department of Technology ("CDT"), issued a Joint Communiqué (Bulletin # P-09-17) requiring "all State Departments to immediately discontinue the use of Kaspersky Labs cybersecurity and information technology products and suspend all procurement activities of these products until further notice."[56] The Bulletin further states: "DGS and CDT strongly urge that the Judicial and Legislative branches, along with Constitutional Officers, comply with this bulletin and confirm their current status with CDT." Finally, the Bulletin states: "In addition, Kaspersky Lab products will be removed from all statewide leveraged procurement vehicles until further notice." The Bulletin states that these actions were done "[c]onsistent with this federal action [by GSA] and in order to protect the integrity and security of the state's information systems and assets."

---

[52] Exhibit 38 (Senate Select Committee on Intelligence, *Hearing on World Wide Threats*, 11 May 2017 (unpaginated excerpt of transcript obtained from Bloomberg Government).

[53] Exhibit 39 (House Committee on Science, Space, & Technology, *SST Committee Probes Kaspersky Lab In Cabinet Level Request*, Press Release, 28 July 2017, https://science.house.gov/news/press-releases/sst-committee-probes-kaspersky-lab-cabinet-level-request).

[54] *See, e.g.*, Exhibit 40 (Adam Mazmonian, *Kaspersky axed from governmentwide contracts*, FCW, 12 July 2017, https://fcw.com/articles/2017/07/12/kaspersky-gsa-nasa-intel.aspx).

[55] Exhibit 40 (Adam Mazmonian, *Kaspersky axed from governmentwide contracts*, FCW, 12 July 2017, https://fcw.com/articles/2017/07/12/kaspersky-gsa-nasa-intel.aspx).

[56] Exhibit 41 (Department of General Services Procurement Division and California Department of Technology Statewide Technology Procurement Division, *Joint Communiqué to Purchasing Authority Contacts, Procurement and Contracting Officers, Chief Information Officers, and Agency Information Officers Regarding Kaspersky Anti-Virus Software*, Bulletin # P-09-17, 18 July 2017, https://www.documents.dgs.ca.gov/pd/delegations/broadcastbulletins/2017/pac071817_P-09-17.pdf).

IV. CLASSIFIED MATERIAL

Enclosed is a classified annex that provides classified evidence relevant to BOD-17-01.

V. ANALYSIS OF UNCLASSIFIED EVIDENCE

Based on the unclassified evidence discussed above, it is clear that the presence of Kaspersky-branded products on U.S. government information systems presents various significant information security risks. These risks arise because of the inherent functionality of anti-virus software, as well as Kaspersky services that present other information security risks, combined with the cybersecurity and national security threat to federal information and information systems posed by the Russian government and its ability to leverage Kaspersky-branded products for intelligence collection or other malicious cyber activities against U.S. government information systems. These risks exist regardless of whether Kaspersky-branded products have already been used by Kaspersky or the Russian government for malicious purposes. Rather, it is the ability for the Russian government or Kaspersky, on behalf of the Russian government, to capitalize on the access to federal information and information systems provided by Kaspersky-branded products, to engage in malicious conduct, that presents sufficient "known or reasonably suspected" information security risks to justify issuance of BOD 17-01.

Like all anti-virus products and other products and solutions that contain anti-virus functionality, Kaspersky software has broad access to files on the hosts on which the software is installed. The NCCIC Assessment documents the significant information security risks raised by anti-virus software generally and Kaspersky-branded products in particular. And the experts cited above concur that anti-virus software functions by repeatedly scanning every file and process on a computer.

In addition, if Kaspersky government customers participate in the Kaspersky Security Network ("KSN"), then an extensive set of data, including whole files or components of files, is eligible for transmission, at Kaspersky's discretion, to Kaspersky servers. The data then is subject to potential access by the FSB, for example, if Kaspersky is compelled to or agrees to provide the FSB with access, if the FSB seconds an agent to work at Kaspersky (overtly or under cover), or if the FSB intercepts the data transmission while it transits Russian networks pursuant to its SORM capabilities. Kaspersky also could target specific files for collection by writing anti-virus signatures that search for specific data or files on federal information systems and that data is transmitted, ostensibly for purpose of further analysis, to Kaspersky servers located in Russia or accessible by Kaspersky analysts in Russia.

Beyond this potential for data exfiltration to Russia, Kaspersky software, like all software, receives signature updates and other software patches, updates and upgrades. This update process provides a means through which Kaspersky or the Russian government could install malware on customer computers. This malware could enable remote access to the computer, data exfiltration, impairment of data integrity, or a wide range of other information security risks.

A wealth of public evidence illustrates that Russia is a significant cybersecurity threat to the U.S. government agencies' information and information systems. This is evident in the statements in

the most recent Worldwide Threat Assessment of the Intelligence Community about Russian malicious cyber activities and media reports of Russian cyber intrusions into the State Department and White House. The history of Russian cyber operations indicate that Russia will seek to use any available means to engage in intelligence collection or other malicious cyber activities. Those means could include leveraging vulnerabilities provided by the installation or presence of Kaspersky products on U.S. government information systems.

This Russian threat presents information security risks regardless of whether or not Kaspersky provides assistance to the FSB or another Russian government agency. Kaspersky could provide such assistance voluntarily (e.g., because of friendships or other ties between Mr. Kaspersky or other Kaspersky officials and intelligence officials) or because Kaspersky is obligated under Russian law to assist the FSB in the execution of the FSB's duties, including the collection of foreign intelligence. If Kaspersky qualifies as a provider of "electronic communications services of all types," the Kaspersky would be obligated to modify its hardware and/or software to implement FSB "operational/technical measures." In addition, with Kaspersky's consent, the FSB could second agents, undercover or overtly, to Kaspersky, to act in furtherance of FSB objectives.

Because Kaspersky needs government licensing and certificates to operate, Russian government agencies may request or require that Kaspersky take action(s) that support Russian government objectives, such as providing the key to decrypt encrypted data transmissions or providing other access to customer data, as a condition of granting needed licenses or certificates. The certificates discussed above suggest that Kaspersky, at least at the time, either was an FSB unit, was part of an FSB unit, or collaborated with an FSB unit.

Even if Kaspersky is not currently explicitly assisting Russian government agencies, the FSB and other agencies still could exploit Kaspersky software for government purposes. As described above, the Russian SORM requires that telecommunications companies and ISPs install equipment that permits FSB remote monitoring of all data transmitted on those networks, which presumably includes data transmitted to and from Kaspersky's headquarters in Moscow, through a Russian internet service provider, through other third party infrastructure, and ultimately to and from Kaspersky's U.S. government customers.

Finally, according to experts, the Russian Government has other ways to influence Kaspersky and its employees, such as by threats to their families and assets.

DHS's concern about Kaspersky access to sensitive information and information systems is consistent with concerns raised by a range of other government actors, including the heads of five intelligence agencies and the General Services Administration.

VI. ANALYSIS OF AVAILABLE CONTRARY EVIDENCE

DHS has considered available contrary evidence, in the form of numerous public statements made by Kaspersky and its representatives in response to concerns raised about the company's products and its ties to the Russian government. Many of these statements are belied by

publicly-available evidence, and both individually and as a whole, they do not sufficiently address the principal concerns motivating the BOD.

A. Asserted Lack of Ties or Assistance to the Russian Government.

Kaspersky has stated that (1) Kaspersky Lab and its executives have no ties to any government; (2) the company has never helped, nor will help, any government in the world with its cyberespionage efforts; and (3) the company has never received a request from the Russian government, or any affiliated organization, to create or participate in any secret projects; and (4) Kaspersky products do not allow any access or provide any private data to any county's government..[57] According to a *Wired* article from 2012, Mr. Kaspersky also stated specifically that the FSB has never made a request to tamper with his software, nor has it tried to install agents in his company.[58]

Kaspersky's claim that Kaspersky and its executives have no ties to any government is disingenuous. Mr. Kaspersky studied at an institute sponsored by the KGB and other government agencies and had a former position with the Ministry of Defense. He also goes to group saunas with individuals that appear to include Russian intelligence officials, and which he has described as "friends."[59] Kaspersky's Chief Operating Officer started his career at a research institute of the Russian Ministry of Defense. Product certificates from 2007 and 2011 also indicate that Kaspersky engaged in some activity as an FSB unit, as part of an FSB unit, or in collaboration with an FSB unit. When asked about the certificates, McClatchy stated that Kaspersky's response did not directly address the reference to an FSB military unit number in several Kaspersky certificates.[60]

B. Customer Control Over Data.

Kaspersky has stated that the risk of data exfiltration can be addressed by customers not participating in KSN, implementing an on-premise KSN, making configuration and security setting changes, or effecting other fixes.[61]

---

[57] Exhibit 42 (Kaspersky Lab response clarifying the inaccurate statements published in a *Bloomberg Businessweek* article on July 11, 2017, Response to No. 3, https://usa.kaspersky.com/about/press-releases/2017_kaspersky-lab-response-clarifying-inaccurate-statements-published-in-bloomberg-businessweek-on-july-11-2017); Exhibit 43 (Kaspersky Lab Press Release, 9 May 2017, https://usa.kaspersky.com/about/press-releases/2017_may-9-2017-statement-regarding-recent-false-allegations-about-kaspersky-lab).

[58] Exhibit 23 (Noah Shachtman, *Russia's Top Cyber Sleuth Foils US Spies, Helps Kremlin Pals*, Wired, 23 July 2012, https://www.wired.com/2012/07/ff_kaspersky/all/).

[59] Exhibit 20 (Jordan Robertson, *A Russian Cybersecurity Company's Ties to the Kremlin*, Bloomberg Technology, 11 July 2017, https://www.bloomberg.com/news/articles/2017-07-11/a-russian-cybersecurity-company-s-ties-to-the-kremlin); Exhibit 24 (Carol Matlack, Michael Riley, Jordan Robertson, *The Company Securing Your Internet Has Close Ties to Russian Spies*, Bloomberg Businessweek, 19 March 2015, updated 20 March 2015, https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies).

[60] Exhibit 19 (David Goldstein and Greg Gordon, *Documents could link Russian cybersecurity firm Kaspersky to FSB spy agency*, McClatchy Washington Bureau, 3 July 2017, http://www.chicagotribune.com/news/nationworld/ct-kaspersky-cyber-russia-spy-agency-20170703-story.html).

[61] *See* Exhibit 43 (Kaspersky Lab Press Release, 9 May 2017, https://usa.kaspersky.com/about/press-releases/2017_may-9-2017-statement-regarding-recent-false-allegations-about-kaspersky-lab); Exhibit 44 (Thomas Fox-Brewster, *Kaspersky Anti-Virus Can Actually Help Spies Steal Data, Warn Researchers*, Forbes, 27 July 2017,

NCCIC has reviewed these statements and determined that, even if all of Kaspersky's statements are fully accurate, information security risks remain. As stated in the NCCIC Assessment, for example, the on-premise version of KSN presumably still requires software updates from Kaspersky, which could include malware or not include all updates needed to identify known cybersecurity threats. In addition, if endpoints require connection with a central on-premise update server and the endpoint is a laptop or other device that is disconnected from the local network for periods of time, that endpoint would likely not receive needed signature updates until it reconnects with the local update server. Thus, use of an on-premise solution introduces risks for devices not connected to the local network.

C. Anonymization of Customer Data.

Kaspersky has stated that it does not gather "identifying data from customers' computers" because it is "technically impossible."[62] The KSN Statement referenced above also states: "Any stored data will not be associated with any personally identifiable information. Kaspersky Lab does not combine the data stored by Kaspersky Security Network with any data, contact lists, or subscription information that is processed by Kaspersky Lab for promotional or other purposes." The KSN Statement states further: "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."[63]

If a customer participates in KSN, it appears that Kaspersky obtains "original information" and retains that information for one year, apart from any anonymized, aggregated "use" of that data. As explained in the NCCIC Assessment, that information could contain a range of data that identifies the customers, such as user account names, computer names, and file paths, even if not combined with subscription information or contact lists. This also could occur, for example, if Kaspersky obtained a quarantined email sent to the customer. Even if a customer does not participate in KSN, Kaspersky still has the ability, even if never exercised, to use a software update to install malicious code on customer computers that could be used to obtain identifying data from the customers' computers.

D. NIST Certification.

Kaspersky has pointed to a National Institute of Standards and Technology ("NIST") certification as evidence that its products are secure. Specifically, Kaspersky states in a press

---

https://www.forbes.com/sites/thomasbrewster/2017/07/27/kaspersky-av-hack-with-satellite-malware/#14a6a9612e0f); Exhibit 45 (Itzik Kotler and Amit Klein, *The Adventures of AV and the Leaky Sandbox*, Presentation to BlackHat USA 2017, slide 42, https://www.blackhat.com/docs/us-17/thursday/us-17-Kotler-The-Adventures-Of-Av-And-The-Leaky-Sandbox.pdf).

[62] Exhibit 42 (Kaspersky Lab response clarifying the inaccurate statements published in a *Bloomberg Businessweek* article on July 11, 2017, Response to No. 8, https://usa.kaspersky.com/about/press-releases/2017_kaspersky-lab-response-clarifying-inaccurate-statements-published-in-bloomberg-businessweek-on-july-11-2017).

[63] Exhibit 6 (Kaspersky Security Network Statement for Kaspersky Endpoint Security 10 for Windows, Section B, http://support.kaspersky.com/9365#block0).

release: "Kaspersky Lab routinely attains licenses and certifications from the countries it operates in, including one from the U.S. National Institute of Standards and Technology, certifying the company's encryption technologies for businesses as fully compliant with the Federal Information Processing Standards (FIPS) 140-2. These certifications and licenses demonstrate Kaspersky Lab products are trusted to secure sensitive data and are protecting organizations without any issues or unexpected behaviors."[64]

A certification of Kaspersky "encryption technologies" as FIPS 140-2 compliant means that the encryption meets the specified standard; it does not mean that NIST reviewed the product for all possible information security issues.

E. Offer to Review Source Code.

Kaspersky has offered its source code for review by the U.S. government.[65]

As described in the NCCIC Assessment, the value of such a review should be viewed with caution. First, by its inherent nature, anti-virus software has broad access rights and privileges, and it is this inherent functionality, when exploited by a malicious actor, that presents information security risks. Thus, even if a source code review found no "backdoors" or other unusual code, these risks would remain. Apart from the inherent risks in the code (when exploited by a malicious actor), if a reviewer did review the code, the reviewer may not know or be able to confirm whether the source code provided is complete and unaltered. The code could also be updated at any time. As stated by Robert Anderson, a former FBI Executive Assistant Director: "[Y]ou have to look at whether that's really what he's giving us. . . . Not everything is as it appears."[66]

F. Offer to Answer Questions or Provide Information to the U.S. Government.

Mr. Kaspersky has offered to testify in a Senate hearing and appears otherwise to welcome the opportunity to provide additional information to the U.S. government regarding concerns about Kaspersky products.[67]

---

[64] Exhibit 43 (Kaspersky Lab Press Release, 9 May 2017, https://usa.kaspersky.com/about/press-releases/2017_may-9-2017-statement-regarding-recent-false-allegations-about-kaspersky-lab).

[65] *See, e.g.*, Exhibit 46 (Raphael Satter and Veronika Silchenko, *Russian anti-virus CEO offers up code for US govt scrutiny*, The Associated Press, 2 July 2017, https://www.apnews.com/37f7f26c48ec4c31bd01ed24704aaba6/Russian-anti-virus-CEO-offers-up-code-for-US-govt-scrutiny).

[66] Exhibit 5 (The Rachel Maddow Show, Russian Kaspersky Lab faces new scrutiny, suspicion, On assignment with Richard Engel, 28 July 2017, 14:40-14:58, http://www.msnbc.com/rachel-maddow/watch/russian-kaspersky-labs-faces-new-scrutiny-suspicion-1012640835507).

[67] *See, e.g.*, Exhibit 47 (Reddit, *I'm Eugene Kaspersky, cybersecurity guy and CEO of Kaspersky Lab! Ask me Anything!*, 11 May 2017, https://www.reddit.com/r/IAmA/comments/6ajstf/im_eugene_kaspersky_cybersecurity_guy_and_ceo_of/?limit=500) (question from "revsehi" and response from "e_kaspersky"); Exhibit 43 (Kaspersky Lab Press Release, 9 May 2017, https://usa.kaspersky.com/about/press-releases/2017_may-9-2017-statement-regarding-recent-false-allegations-about-kaspersky-lab).

Kaspersky will have an opportunity, through an administrative process that DHS is making available to Kaspersky and other entities whose commercial interests are directly impacted by the BOD, to submit additional information and arguments to DHS. The Department should remain open to hearing new information, review any such submission(s) closely, and adjust its analysis to the extent warranted.

VII. RECOMMENDATION

Based on the unclassified evidence alone, Kaspersky-branded products present known or reasonably suspected information security risks to U.S. government information and information systems, and you should issue BOD 17-01 based on the unclassified record. Classified information further supports this action.

Exhibit 4.A

U.S. Department of Homeland Security
National Cybersecurity and Communications Integrations Center

Information Security Risk Assessment:

COTS Antivirus Software and Kaspersky-Branded Products

August 29, 2017

NCCIC

PURPOSE

This assessment presents the inherent information security concerns and security ramifications associated with the use of any commercial-off-the-shelf (COTS) antivirus solution in devices with access to a federal network. It also addresses specific risks presented by Kaspersky-branded products, solutions, and services (collectively, "Kaspersky-branded products").

BACKGROUND

Many organizations deploy antivirus software solutions to user workstations as a base layer of security to detect and remove the most common threats, including Trojans, malware, worms, and adware. Antivirus solutions have become a default part of cyber hygiene at the workstation level, though security experts recommend antivirus software be deployed alongside a full security stack to more robustly protect the network, a practice referred to as layered security or "defense-in-depth."[1]

Antivirus solutions usually employ one or more of three signature detection methods: file scanning, heuristics, and emulation.[2] File scanning leverages full content inspection in order to detect malicious code in files downloaded, emailed, or transferred to the computer. Heuristic scanning monitors all processes and establishes baselines for a workstation's patterns of behavior in order to detect deviations from those baselines. Emulators use sandboxed virtual machines to test run suspicious or encrypted executables. Monitoring changes in the sandbox allows the antivirus software to make a determination of whether the suspicious process is safe to execute on the host system or if the process is deemed unsafe and should be deleted or quarantined.

In order to perform these functions and protect the workstation, antivirus software requires the highest level of system privileges, particularly to combat any malicious software that might try to remove the antivirus or interrupt kernel-level system calls as part of its attack kill-chain. Each antivirus product operates off an antivirus engine—the main kernel programmed to search for malicious activity using the methods described above. Multiple antivirus products from different antivirus companies may share the same antivirus engine if an antivirus company does not have the resources to build its own engine.[3]

---

1 Shenk, 2013.
2 Sanok Jr, 2005.
3 Koret, 2014.

GENERAL ANTIVIRUS SECURITY CONCERNS

Deploying an antivirus product increases that workstation's attack surface. Mitigating this risk requires:

- trust in the antivirus company not to abuse its privileges on the host; and
- trust in the product to capably resist hijacking by the attackers against which it defends.

Assessing the vendor's reputation for trustworthiness is a crucial part of any security product acquisition process.

In order to perform their basic functions, antivirus products operate with the highest level of system privileges, which is higher than any standard computer process. This gives the antivirus vendor system-level privileges on the customer endpoints it defends. An antivirus product also has full content inspection capabilities, and could remove or transmit anything—from a downloaded Trojan and routine detection metrics to Personally Identifiable Information (PII) and proprietary data—back to its home servers. Because antivirus processes are often white-listed by the other products in an organization's security stack, an immense level of trust is granted to the antivirus vendor not to abuse that level of access for economic, espionage, or destructive purposes.

Many antivirus vendors now provide a virtual machine known as a "cloud sandbox" to further analyze suspicious executables. When the antivirus software detects and quarantines a suspicious file, it uploads the suspicious file to the antivirus vendor's virtual machine sandbox, which is located on a remote server (requiring an upload over the Internet). Some sandboxes are self-contained to prevent malware samples from contacting their command-and-control servers, but others remain connected to the Internet to record and analyze the malware's unhindered execution and communications. Researchers from SafeBreach Labs found it possible to hijack these Internet-connected sandboxes for data exfiltration. They accomplished this by having the malware embed the desired data payload into a second malware sample before purposely triggering the antivirus quarantine function. The antivirus then uploads the data-infused malware to the cloud sandbox, where it can contact and exfiltrate the data to attacker-controlled servers with no interference from the passive sandbox.[4]

Another feature many antivirus products advertise is the capability to "break-and-inspect" Hyper Text Transfer Protocol Secure (HTTPS) traffic for malicious code by intercepting the traffic with a man-in-the-middle (MITM) connection.[5] The antivirus software uses its own certificate to sign outgoing traffic from the user and incoming traffic from the server in order to decrypt the content and determine whether malicious commands or software are part of the communication. However, this technique expands the attack surface further, because it leaves no way for the

[4] Klein and Kotler, 2017.

[5] Bachaalany and Koret, 2015.

client to independently validate its connection to the server and leaves it wholly dependent on the security product's validation.[6]

Additional concerns lie in flaws with the antivirus products themselves, as some "do not properly verify the certificate chain of the server,"[7] do not always forward certificate-chain verification errors to the client, and occasionally connect to servers using weaker encryption protocols than the client itself would allow.[8] Even with the antivirus product working securely, simply employing this function defeats the purpose of end-to-end encrypted HTTPS connections with an external server because a third party is allowed to read, manipulate, and forward any information in the connection. In the best case, an antivirus product would detect an encrypted malware callback and remove it from the outgoing traffic so the malware cannot contact the attacker's server. In the worst case, a product could store and exfiltrate sensitive information, including login credentials being transmitted from the client to the server, or otherwise compromise the integrity of the network communication.

Furthermore, any software that receives vendor-provided updates could disguise known malicious software via the antivirus update process. Just as antivirus companies like Webroot have accidentally released signature updates that mistakenly identify legitimate programs as malicious,[9] an antivirus company could just as easily provide signatures marking known malicious software as legitimate and safe. More subtly, the antivirus software could withhold signatures that would identify known malware. Additionally, even a correctly functioning antivirus update process can still fall victim to third-party attack, as Windows Update did in 2012 when the Flame virus spoofed a legitimate Microsoft certificate to trick the workstation into loading the malware launcher, which was disguised as a normal update.[10] While antivirus definitions are usually specially formatted and encrypted lists of pattern-match signatures, updates to the antivirus software itself modify the code the program runs on, and the updates themselves could potentially include malicious code.

Deployment of personal antivirus on employee bring-your-own-devices (BYOD) introduces additional security considerations because, while these devices are not subject to the same supplementary security restrictions and access controls as an enterprise workstation, they are often allowed to operate on the same enterprise data.

Like any software, antivirus products themselves are subject to exploitation, and any attacker with the ability to compromise the product has the ability to assume the security privileges of that running process. COSEINC security researcher and author of *The Antivirus Hacker's Handbook*, Joxean Koret presented multiple vulnerabilities, identified across a wide array of

[6] US-CERT, 2017.
[7] US-CERT, 2017.
[8] US-CERT, 2017.
[9] Sulleyman, 2017.
[10] Whitney, 2012.

different antivirus products, during his presentation to the information security conference 44CON in 2014.

While many of these security flaws were quickly patched by the antivirus companies in question, Koret also identified vulnerabilities inherent to using any commercial antivirus engine, such as:

- buffer overflows due to the properties of the programming languages used to code most engines;
- virus definition updates sent over HTTP and vulnerable to MITM attacks;
- libraries compiled without using address space layout randomization (ASLR); and
- other vulnerabilities.[11]

A security stack is only as strong as its weakest component, and antivirus solutions present a large vulnerability in the event that an attacker can compromise the software.

KASPERSKY-SPECIFIC CONSIDERATIONS

Based on publicly available information, Kaspersky-branded antivirus software and other Kaspersky-branded products and solutions that contain antivirus functionality appear to present the general antivirus software risks identified above. For example, the default installation of Kaspersky Internet Security scans all encrypted HTTPS connections using the interception technique described above in order to detect malicious activity.[12]

Additionally, Kaspersky customers may participate in the Kaspersky Security Network (KSN). KSN is a cloud-based network to which a wide range of data from customer devices may be transferred for the purpose of additional analysis. A list of such data is available in the KSN Statement, which users must agree to in order to participate.[13] Under the terms of the agreement, the information subject to transfer includes highly sensitive data collected from a user's device, such as information about the computer's hardware and software, files downloaded, certain websites visited, running applications, and user account names—essentially the full spectrum of forensic data a device produces. Furthermore, Kaspersky notes in the KSN Statement that it reserves the right to disclose any of the information processed "under confidentiality and licensing agreements with certain third parties which assist [Kaspersky] in developing, operating, and maintaining the Kaspersky Security Network."[14] These third parties may be trusted partners of Kaspersky, but that does not mean they are subject to the same vetting and rigorous suitability scrutiny as other companies with which the U.S. Government has entrusted its data.

[11] Koret, 2014.
[12] Kaspersky Labs 2017.
[13] Kaspersky Labs 2017.
[14] Kaspersky Labs 2017.

Kaspersky also notes that "no data transmission can be guaranteed secure"[15] and "[Kaspersky] cannot guarantee the security of any data [participants] transmit to [Kaspersky] or from [Kaspersky] products or services,"[16] with a final warning that participants "use all these services at [their] own risk."[17] Such data, whether provided to Kaspersky through normal course of operation, to third parties by Kaspersky as part of their sharing agreement, or to adversaries by in-transit interception techniques, could assist an attacker in obtaining sensitive files from government computers, targeting employees with precisely crafted spear-phishing attacks, and other information security risks.

Kaspersky has made statements that the risks of KSN can be mitigated by the customer or user. A May 9, 2017, Kaspersky press release states: "Unlike in many other products, Kaspersky Lab users have full control over telemetry (data) sharing with their participation being voluntary, and they can disable telemetry reporting completely at any given time. In addition, business and government users may choose to install a local and private Kaspersky Security Network (KSN) center on their premises to make sure the data never leaves their facility."[18]

The National Cybersecurity and Communications Integration Center (NCCIC) recognizes that Kaspersky may offer customers the ability to deploy a KSN center on the customer's local network and choose configuration settings that limit or eliminate the transfer of data to the KSN (among other potential options). However, assuming that the statements made by Kaspersky are fully accurate and it is possible to prevent any files from leaving a host or network, that assumption still does not address threats posed by the software itself as an on-premise solution. The level of system access granted to antivirus software would allow malicious activity to be conducted through the antivirus software itself, and even if the threat is not present in a current build of the software, it could be added through a future update or a third-party exploitation of the software. In order to stay up-to-date with the most advanced threats, even on-premise solutions require vendor updates to the antivirus signatures and less frequent updates to the software itself; and these updates are usually downloaded via temporary or indirect Internet connection or physical media like USB flash drives. Any software update has the potential to add functionality or expand the attack surface of the host machine. If a vendor withheld a signature update, the endpoints would remain vulnerable to a known threat. Furthermore, while the customer has the option of making configuration changes in the antivirus software, a configuration page is only a user interface, meaning it could display options as disabled while they remain enabled in the antivirus code.

Kaspersky also offers various cybersecurity services, including threat hunting, incident response, and security assessment. The information security risk presented by any service depends on the

[15] Kaspersky Labs 2017.
[16] Kaspersky Labs 2017.
[17] Kaspersky Labs 2017.
[18] Kaspersky 2017.

specifics of the service provided. In general, these services present various significant information security risks. For example, 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.

RECOMMENDATIONS

While new software acquisitions are primarily assessed for technical capability, effectiveness, and ease of use, vendors should undergo vetting separate from that of their products. Security vendors with access to sensitive federal data and networks must be confirmed as trustworthy partners who keep customer business independent of—and unaffected by—any obligations to the vendors' home government or commercial partners.

In response to concerns about the security of an antivirus product, some vendors may offer a government the opportunity to review the product's source code. The value of such a review should be viewed with caution. First, by its inherent nature, antivirus software has broad access rights and privileges (as described above), and it is this inherent functionality that presents information security risks. Thus, even if a source code review found no backdoors or other unusual code, these risks would remain. Apart from the inherent risks in the code (when exploited by a malicious actor), if a reviewer did review the code, the reviewer may not know or be able to confirm whether the provided source code is complete and unaltered. The code could also be updated at any time, and the reviewing party may not have the resources or ability to continually re-review the code. The review also may be incomplete or ineffective unless done by someone with deep familiarity with the software (such as one of its original developers).

WORKS CITED

Bachaalany, Elias, and Joxean Koret. “The Antivirus Hacker's Handbook”. Indianapolis: John Wiley & Sons, Inc., 2015.

Kaspersky Labs. "Kaspersky Internet Security 2018 release notes: commercial release of version 18.0.0.405." Kaspersky. August 14, 2017. http://support.kaspersky.com/13617#block1 (accessed August 18, 2017).

Kaspersky Labs. "Kaspersky Security Network Statement." Kaspersky. March 3, 2017. http://support.kaspersky.com/9365#block0 (accessed August 8, 2017).

Kaspersky. May 9, 2017 Statement Regarding Recent False Allegations about Kaspersky Lab. May 9, 2017. https://usa.kaspersky.com/blog/statement-regarding-false-allegations/11109/ (accessed August 23, 2017).

Klein, Amit, and Itzik Kotler. "The Adventures of AV and the Leaky Sandbox." SafeBreach. July 28, 2017. https://go.safebreach.com/rs/535-IXZ-934/images/Adventures_AV_Leaky_Sandbox.pdf (accessed August 23, 2017).

Koret, Joxean. "Breaking Antivirus Software." 44CON. 2014. 146. http://joxeankoret.com/download/breaking_av_software_44con.pdf (accessed August 18, 2017).

Sanok Jr., Daniel J. "An Analysis of How Antivirus Methodologies Are Utilized in Protecting Computers from Malicious Code." InfoSecCD '05 Proceedings of the second annual conference on Information security curriculum development. Kennesaw, GA: ACM New York, NY, USA, 2005. 142-144.

Shenk, Jerry. Layered Security: Why It Works. White Paper, SANS Institute, 2013. https://www.sans.org/reading-room/whitepapers/analyst/layered-security-works-34805 (accessed August 27, 2017).

Sulleyman, Aatif. "Windows Users Mystified As Antivirus Accidentally Cripples Computers." The Independent. April 25, 2017. http://www.independent.co.uk/life-style/gadgets-and-tech/news/windows-antivirus-software-malware-webroot-trojan-facebook-microsoft-a7701896.html (accessed August 18, 2017).

US-CERT. "HTTPS Interception Weakens TLS Security." National Cyber Awareness System (NCAS) Alert (TA17-075A). March 16, 2017. https://www.us-cert.gov/ncas/alerts/TA17-075A (accessed August 24, 2017).

Whitney, Lance. Flame virus can hijack PCs by spoofing Windows Update. June 5, 2012. https://www.cnet.com/news/flame-virus-can-hijack-pcs-by-spoofing-windows-update/ (accessed August 24, 2017).

Exhibit 5

September 13, 2017

Kaspersky Lab Response to Issuance of DHS Binding Operational Directive 17-01

Given that Kaspersky Lab doesn't have inappropriate ties with any government, the company is disappointed with the decision by the U.S. Department of Homeland Security (DHS), but also is grateful for the opportunity to provide additional information to the agency in order to confirm that these allegations are completely unfounded.

Woburn, MA – September 13, 2017 – "Given that Kaspersky Lab doesn't have inappropriate ties with any government, the company is disappointed with the decision by the U.S. Department of Homeland Security (DHS), but also is grateful for the opportunity to provide additional information to the agency in order to confirm that these allegations are completely unfounded. No credible evidence has been presented publicly by anyone or any organization as the accusations are based on false allegations and inaccurate assumptions, including claims about the impact of Russian regulations and policies on the company. Kaspersky Lab has always acknowledged that it provides appropriate products and services to governments around the world to protect those organizations from cyberthreats, but it does not have unethical ties or affiliations with any government, including Russia.

"In addition, more than 85 percent of its revenue comes from outside of Russia, which further demonstrates that working inappropriately with any government would be detrimental to the company's bottom line. These ongoing accusations also ignore the fact that Kaspersky Lab has a 20-year history in the IT security industry of always abiding by the highest ethical business practices and trustworthy technology development.

"Regarding the Russian policies and laws being misinterpreted, the laws and tools in question are applicable to telecom companies and Internet Service Providers (ISPs), and contrary to the inaccurate reports, Kaspersky Lab is not subject to these laws or other government tools, including Russia's System of Operative-Investigative Measures (SORM), since the company

doesn't provide communication services. Also, it's important to note that the information received by the company, as well as traffic, is protected in accordance with legal requirements and stringent industry standards, including encryption, digital certificates and more.

"Kaspersky Lab has never helped, nor will help, any government in the world with its cyberespionage or offensive cyber efforts, and it's disconcerting that a private company can be considered guilty until proven innocent, due to geopolitical issues. The company looks forward to working with DHS, as Kaspersky Lab ardently believes a deeper examination of the company will substantiate that these allegations are without merit." – **Attributable to Kaspersky Lab**

Articles related to Press Releases

Kaspersky Lab Remains Committed to the North American Market

The company continues to invest in North American market; will be opening three new regional offices in 2018

>

Kaspersky Lab response clarifying the inaccurate statements published in a New York Times op-ed on September 4, 2017

>

NMW2017: Kaspersky Lab and AVL Software and Functions GmbH pave the way for secure-by-design connected cars

FRANKFURT, Germany – September 13, 2017 – In response to the rising cybersecurity challenges facing the connected and autonomous car industry, today Kaspersky Lab and AVL Software and Functions GmbH unveil the Secure

Exhibit 6

Principles for the processing of user data by Kaspersky Lab security solutions and technologies

Respecting and protecting people's privacy is a fundamental principle of Kaspersky Lab's approach to processing users' data. The data that is processed is crucial for identifying new and as yet unknown threats – such as WannaCry and ExPetr – and offering better protection products to users. Analyzing big data from millions of devices to strengthen protection capabilities is an industry best practice that is applied by IT security vendors around the world. It is a must for securing users' digital lives from cyberthreats.

Details of the data processed can be found in the End-User License Agreement (EULA) and the Kaspersky Security Network (KSN) Agreement (which differ depending on the product). This data includes information about the device (such as device type, operating system, etc.), any threats detected on it, suspicious events in the operating system, etc. The information is used in the form of aggregated statistics in separated systems with strict policies regarding access rights, and we do not attribute data to specific individuals.

Users of Kaspersky Lab products can reduce the amount of data processed from their protected devices to the absolute minimum. All data processed and/or transferred is robustly secured through encryption, digital certificates, segregated storage and strict data access policies.

The main principles

- Information processed in the company's cloud-based systems is crucial for protecting users from the newest and most sophisticated threats.
- This information is limited to what is needed in order to improve detection algorithms, refine the products' operation and offer better solutions to our customers.
- Data sent to Kaspersky Lab is not attributed to a specific individual. The information is used as aggregated statistics, on separated servers with strict policies regarding access rights.
- Kaspersky Lab is committed to anonymizing information wherever possible, and actions to achieve this include deleting account details from transmitted URLs, obtaining hash sums of threats instead of the exact files, obscuring user IP addresses etc.
- Users have control over the amount of data being shared, because participation in Kaspersky Security Network is voluntary and can be disabled at any time. If users disable KSN, a small amount of data that is essential for the product to function

- The information shared is protected, even during transit in accordance with stringent industry standards, including through encryption, digital certificates, and more.
- Kaspersky Lab constantly reviews the type of data processed by its solutions to protect our customers' privacy and comply with the very latest legal requirements, such as the upcoming GDPR regulations in Europe.

What is Kaspersky Security Network?

Kaspersky Security Network (KSN) is one of Kaspersky Lab's main cloud systems that was created to maximize the effectiveness of discovering new and unknown cyberthreats and thereby ensure the quickest and most effective protection for users. KSN is an advanced cloud-based system that automatically processes cyberthreat-related data received from millions of devices owned by Kaspersky Lab users across the world, who have voluntarily opted to use this system. This cloud-based system approach is now the industry standard, applied by many global IT security vendors.

What is a 'cloud'-based system'?

This is a system that runs on a company's servers rather than on individual devices and which can be used over the internet from anywhere in the world. Examples of cloud systems include email, file sharing and file hosting systems. Kaspersky Lab's cloud servers are distributed across the globe (e.g. in Germany, China, Canada, Russia etc.), enabling faster processing of information and guaranteeing server availability should one of them fail for any reason.

What is the purpose of cloud-based protection?

Most IT security vendors use the cloud to improve protection levels, and a hybrid protection model (antivirus databases + proactive defense + the cloud) is the most effective.

The high performance capability of corporate servers means that cyberthreats detected on user devices can be analyzed faster and more accurately. While the traditional antivirus and anti-phishing database updating cycle usually takes several hours, the cloud can provide users with protection against a new threat within minutes.

Using the cloud can also make a security product 'lighter' by keeping it from taking up too much memory and resources on the user device.

Why should I accept the KSN agreement and share statistics with

The more users there are that contribute to the cloud intelligence, the better the protection will be for all users. Electing to opt out of sharing information with the Kaspersky Security Network (KSN) impacts how quickly the product can react to new and emerging cyberthreats. Home users not sharing data with KSN will not lose cloud protection, but if many choose this option, the overall level of security will inevitably be affected in the long run. If a corporate user opts out of KSN, it means that they will not be able to receive cloud protection at all. In this case, companies can apply an additional layer of protection – Kaspersky Private Security Network, which allows them to get the advantages of cloud protection without any data leaving the company's facility.

Can the data transfer be restricted?

Yes, users have control over the amount of data being shared, because participation in Kaspersky Security Network is voluntary and can be disabled at any time. If users disable KSN, a small amount of data will be shared that is essential for the product to function properly.

The transfer of such information – for example, device, product and license information – is necessary in home or corporate products. This data is used to identify legitimate products, send them database updates, keep them operational, etc. This obligatory information is listed in **the End-User License Agreement.**

For home users, this list also includes websites visited, information on Wi-Fi access points and threats detected. These are necessary for offering a higher level of protection to users, such as enabling the Wi-Fi reputation feature that allows dangerous and fake Wi-Fi hotspots to be identified.

The Kaspersky Security Network agreement contains a list of data that customers can opt out of sharing at any time by unchecking the corresponding box in the product settings (they can also reverse this decision whenever they choose). Should they decide to disable KSN, corporate clients will be unable to receive urgent threat detections made in the cloud. In order to address this, Kaspersky Lab has developed Kaspersky Private Security Network for corporate clients, which allows them to get the advantages of cloud protection without any data leaving the company facility.

The volume and structure of information sent varies by product and is explained in each product's agreement. Please follow this link for more information.

Do you process personal data?

Different laws define personal data differently. For example, GDPR says that 'personal data' means any information relating to an identified or identifiable natural person ('data subject'). In its turn, international standard ISO/IEC 29100:2011(E) says that personally identifiable information (PII) is any information that can be used to identify the PII principal to whom such information relates, or might

In accordance with the new legal frameworks being introduced in some countries, information processed in Kaspersky Lab's cloud may contain data that might be considered as personal or personally identifiable. This could be email addresses used to access the My Kaspersky portal, information used to differentiate users' licenses and devices in order to let them work properly, etc. However, we do not attribute this data to a specific person. Further, data is reliably protected with encryption and other security measures, including anonymization methods, and is used only to enable our products and services to work better and to provide users with the highest level of protection.

How do you anonymize the data you process?

Kaspersky Lab takes user privacy extremely seriously. The company implements the following measures to anonymize obtained data:

- The information is used in the form of aggregated statistics;
- Logins and passwords are filtered out from transmitted URLs, even if they are stored in the initial browser request from the user;
- When we process possible threat data, by default we do not use the suspicious file. Instead we use hash-sum, which is a one-way math function that provides a unique file identifier;
- Where possible, we obscure IP addresses and device information from the data received;
- The data is stored on separated servers with strict policies regarding access rights, and all the information transferred between the user and the cloud is securely encrypted.

How do users benefit from data processing in the cloud? What data is processed?

The data obtained for further analysis depends on the product, and it is recommended that users carefully read the agreements accepted during installation. The data includes the following:

- **License/ subscription information**

We are always on hand to support our customers in the case of a cyberattack and our products are no different. License/ subscription data helps us to tailor products to our users and provide them with solutions that are faster and easier to use.

- **Product information**

example, how long does threat scanning take? Which features are used more often than others? Answers to these and other questions help us to send product and antivirus database updates to legitimate users, ensuring they remain protected from the latest threats.

Device data

Related to user experience is convenience, something we are always looking to improve at Kaspersky Lab to make cybersecurity easier for our customers. Data such as device type, operating system, etc. is needed to identify a specific computer or phone. Matching a license to a specific device means the user doesn't have to buy a new license for the security product after reinstalling the operating system, so they can pick up exactly where they left off.

Threats detected

For users' safety, their cybersecurity solutions should be up-to-date with the latest threats and that is exactly what we provide. Modern cyberthreats are constantly evolving, meaning threat databases need to be regularly updated. If a threat (new or known) is found on a device, information about that threat is sent to Kaspersky Lab. This enables us to analyze threats, their sources, principles of infection, etc., resulting in a higher quality of protection for every user.

Information on installed applications

At Kaspersky Lab, we believe each individual user deserves a personalized experience specific to them. To achieve this, information on installed applications is processed to create lists of 'white' or harmless applications and prevents security products from hindering the user experience by mistakenly identifying such applications as malicious. In addition, this information helps us to offer users security solutions that best match their needs, giving users a greater level of personalization.

URLs visited

We want Kaspersky Lab customers to always have the highest level of protection when they are browsing the web, no matter which websites they visit. So, URLs can be sent to the cloud to check if they are malicious and prevent users from visiting them. This information also helps to create lists of 'white' or harmless websites and prevents security products from mistakenly identifying such websites as malicious and detracting from the user experience. In addition, this information helps us to offer users security solutions that best match their needs. We filter out information regarding logins and passwords from transmitted URLs, even if they are stored in the initial browser request from the user.

Operating System events

of the latest cyberthreats, the product analyzes data on processes running on the device. This makes it possible to identify early on processes that indicate malicious activity, and to quickly prevent any potentially damaging consequences, such as the theft or destruction of user data.

Suspicious files

The analysis of suspicious files helps users to stay protected from the newest and most sophisticated malware. If an (as yet) unknown file exhibiting suspicious behavior is detected on a device, it can be automatically sent to the cloud for a more thorough analysis by machine learning-based technologies and, in rare cases, by a malware analyst. Personal files (such as photos or documents) are rarely malicious and do not behave suspiciously. As a result, the 'suspicious' category includes mainly executable files (.exe).

Wi-Fi connection data

Wi-Fi networks are everywhere these days, but many are not secure. In order to help users feel confident that they are protected wherever they go, Wi-Fi information is analyzed in order to warn users of insecure (i.e., poorly protected) Wi-Fi access points, helping to prevent personal data from being inadvertently intercepted by cybercriminals.

User information

Customers need to know that their accounts are secure and can be accessed from anywhere, so email addresses are used for authorization on the My Kaspersky web portal, which enables users to manage their protection remotely. Email addresses are also used to send targeted messages (e.g., containing important alerts) to users of Kaspersky Lab products. Users can also choose to specify the names (or nicknames) by which they would like to be addressed on the My Kaspersky portal and in emails. Contact information is provided by users at their own discretion.

Dump and trace files

We want Kaspersky Lab users to enjoy a quality user experience so, by checking the special box in the product settings, users can share error reports with Kaspersky Lab servers. This information helps to analyze any errors that might occur in the product and to modify it accordingly so that it will function more effectively moving forward. Users have to manually approve every report before it is sent to the cloud.

Where is this data stored?

Kaspersky Security Network's front-end servers are located in different countries around the world (Germany, Canada, China, Russia, etc.), while the back-end servers are located in Russia, where the

Do you share personal data, processed by Kaspersky Lab solutions, with third parties?

We do not share the information with any third parties.

Exhibit 7

Investigation Report for the September 2014 Equation malware detection incident in the US

By Kaspersky Lab on November 16, 2017. 10:00 am

Background

In early October, a story was published by the Wall Street Journal alleging Kaspersky Lab software was used to siphon classified data from an NSA employee's home computer system. Given that Kaspersky Lab has been at the forefront of fighting cyberespionage and cybercriminal activities on the Internet for over 20 years now, these allegations were treated very seriously. To assist any independent investigators and all the people who have been asking us questions whether those allegations were true, we decided to conduct an internal investigation to attempt to answer a few questions we had related to the article and some others that followed it:

1. Was our software used outside of its intended functionality to pull classified information from a person's computer?
2. When did this incident occur?
3. Who was this person?
4. Was there actually classified information found on the system inadvertently?
5. If classified information was pulled back, what happened to said data after? Was it handled appropriately?
6. Why was the data pulled back in the first place? Is the evidence this information was passed on to "Russian Hackers" or Russian intelligence?
7. What types of files were gathered from the supposed system?
8. Do we have any indication the user was subsequently "hacked" by Russian hackers and data exfiltrated?
9. Could Kaspersky Lab products be secretly used to intentionally siphon sensitive data unrelated to malware from customers' computers?
10. Assuming cyberspies were able to see the screens of our analysts, what could they find on it and how could that be interpreted?

Answering these questions with factual information would allow us to provide reasonable materials to the media, as well as show hard evidence on what exactly did or did not occur, which may serve as a food for thought to everyone else. To further support the objectivity of the internal investigation we ran our investigation using multiple analysts of non-Russian origin and working outside of Russia to avoid even potential accusations of influence.

The Wall Street Journal Article

The article published in October laid out some specifics that need to be documented and fact checked. Important bullet points from the article include:

- The information "stolen" provides details on how the U.S. penetrates foreign computer networks and defends against cyberattacks.
- A National Security Agency contractor removed the highly classified material and put it on his home computer.
- The data ended up in the hands of so called "Russian hackers" after the files were detected using Kaspersky Lab software.
- The incident occurred in 2015 but wasn't discovered until spring of last year [2016].
- The Kaspersky Lab linked incident predates the arrest last year of another NSA contractor, Harold Martin.
- "Hackers" homed in on the machine and stole a large amount of data after seeing what files were detected using Kaspersky data.

Beginning of Search

Having all of the data above, the first step in trying to answer these questions was to attempt to identify the supposed incident. Since events such as what is outlined above only occur very rarely, and we diligently keep the history of all operations, it should be possible to find them in our telemetry archive given the right search parameters.

The first assumption we made during the search is that whatever data was allegedly taken, most likely had to do with the so-called Equation Group, since this was the major research in active stage during the time of alleged incident as well as many existing links between Equation Group and NSA highlighted by the media and some security researchers. Our Equation signatures are clearly identifiable based on the malware family names, which contain words including "Equestre", "Equation", "Grayfish", "Fanny", "DoubleFantasy" given to different tools inside the intrusion set. Taking this into account, we began running searches in our databases dating back to June 2014 (6 months prior to the year the incident allegedly happened) for all alerts triggered containing wildcards such as "HEUR:Trojan.Win32.Equestre.*". Results showed quickly: we had a few test (silent) signatures in place that produced a LARGE amount of false positives. This is not something unusual in the process of creating quality signatures for a rare piece of malware. To alleviate this, we sorted results by count of unique hits and quickly were able to zoom in on some activity that happened in September 2014. It should be noted that this date is technically not within the year that the incident supposedly happened, but we wanted to be sure to cover all bases, as journalists and sources sometimes don't have all the details.

Below is a list of all hits in September for an "Equestre" signature, sorted by least amount to most. You can quickly identify the problem signature(s) mentioned above.

Detection name (silent)	Count
HEUR:Trojan.Win32.Equestre.u	1
HEUR:Trojan.Win32.Equestre.gen.422674	3
HEUR:Trojan.Win32.Equestre.gen.422683	3

HEUR:Trojan.Win32.Equestre.gen.427692 3
HEUR:Trojan.Win32.Equestre.gen.427696 4
HEUR:Trojan.Win32.Equestre.gen.446160 6
HEUR:Trojan.Win32.Equestre.gen.446979 7
HEUR:Trojan.Win32.Equestre.g 8
HEUR:Trojan.Win32.Equestre.ab 9
HEUR:Trojan.Win32.Equestre.y 9
HEUR:Trojan.Win32.Equestre.l 9
HEUR:Trojan.Win32.Equestre.ad 9
HEUR:Trojan.Win32.Equestre.t 9
HEUR:Trojan.Win32.Equestre.e 10
HEUR:Trojan.Win32.Equestre.v 14
HEUR:Trojan.Win32.Equestre.gen.427697 18
HEUR:Trojan.Win32.Equestre.gen.424814 18
HEUR:Trojan.Win32.Equestre.s 19
HEUR:Trojan.Win32.Equestre.x 20
HEUR:Trojan.Win32.Equestre.i 24
HEUR:Trojan.Win32.Equestre.p 24
HEUR:Trojan.Win32.Equestre.q 24
HEUR:Trojan.Win32.Equestre.gen.446142 34
HEUR:Trojan.Win32.Equestre.d 39
HEUR:Trojan.Win32.Equestre.j 40
HEUR:Trojan.Win32.Equestre.gen.427734 53
HEUR:Trojan.Win32.Equestre.gen.446149 66
HEUR:Trojan.Win32.Equestre.ag 142
HEUR:Trojan.Win32.Equestre.b 145
HEUR:Trojan.Win32.Equestre.h 310
HEUR:Trojan.Win32.Equestre.gen.422682 737
HEUR:Trojan.Win32.Equestre.z 1389
HEUR:Trojan.Win32.Equestre.af 2733
HEUR:Trojan.Win32.Equestre.c 3792
HEUR:Trojan.Win32.Equestre.m 4061
HEUR:Trojan.Win32.Equestre.k 6720
HEUR:Trojan.Win32.Equestre.exvf.1 6726
HEUR:Trojan.Win32.Equestre.w 6742
HEUR:Trojan.Win32.Equestre.f 9494
HEUR:Trojan.Win32.Equestre.gen.446131 26329
HEUR:Trojan.Win32.Equestre.aa 87527

HEUR:Trojan.Win32.Equestre.gen.447002 547349
HEUR:Trojan.Win32.Equestre.gen.447013 1472919

Taking this list of alerts, we started at the top and worked our way down, investigating each hit as we went trying to see if there were any indications it may be related to the incident. Most hits were what you would think: victims of Equation or false positives. Eventually we arrived at a signature that fired a large number of times in a short time span on one system, specifically the signature "HEUR:Trojan.Win32.Equestre.m" and a 7zip archive (referred below as "[undisclosed].7z"). Given limited understanding of Equation at the time of research it could have told our analysts that an archive file firing on these signatures was an anomaly, so we decided to dig further into the alerts on this system to see what might be going on. After analyzing the alerts, it was quickly realized that this system contained not only this archive, but many files both common and unknown that indicated this was probably a person related to the malware development. Below is a list of Equation specific signatures that fired on this system over a period of approximately three months:

HEUR:Trojan.Win32.Equestre.e
HEUR:Trojan.Win32.Equestre.exvf.1
HEUR:Trojan.Win32.Equestre.g
HEUR:Trojan.Win32.Equestre.gen.424814
HEUR:Trojan.Win32.Equestre.gen.427693
HEUR:Trojan.Win32.Equestre.gen.427696
HEUR:Trojan.Win32.Equestre.gen.427697
HEUR:Trojan.Win32.Equestre.gen.427734
HEUR:Trojan.Win32.Equestre.gen.446142
HEUR:Trojan.Win32.Equestre.gen.446993
HEUR:Trojan.Win32.Equestre.gen.465795
HEUR:Trojan.Win32.Equestre.i
HEUR:Trojan.Win32.Equestre.j
HEUR:Trojan.Win32.Equestre.m
HEUR:Trojan.Win32.Equestre.p
HEUR:Trojan.Win32.Equestre.q
HEUR:Trojan.Win32.Equestre.x
HEUR:Trojan.Win32.GrayFish.e
HEUR:Trojan.Win32.GrayFish.f

In total we detected 37 unique files and 218 detected objects, including executables and archives containing malware associated with the Equation Group. Looking at this metadata during current investigation we were tempted to include the full list of detected files and file paths into current report, however, according to our ethical standards, as well as internal policies, we cannot violate our users' privacy. This was a hard decision, but should we make an exception once, even for the sake of protecting our own company's reputation, that would be a step on the route of giving up privacy and freedom of all people who rely on our products. Unless we receive a legitimate request originating from the owner of that system or a higher legal authority, we cannot release such information.

The file paths observed from these detections indicated that a developer of Equation had plugged in one or more removable drives, AV signatures fired on some of executables as well as archives containing them, and any files detected (including archives they were contained within) were automatically pulled back. At this point in time, we felt confident we had found the source of the story fed to Wall Street Journal and others. Since this type of event clearly does not happen often, we believe some dates were mixed up or not clear from the original source of the leak to the media.

Our next task was to try and answer what may have happened to the data that was pulled back. Clearly an archive does not contain only those files that triggered, and more than likely contained a possible treasure trove of data pertaining to the intrusion set. It was soon discovered that the actual archive files themselves appear to have been removed from our storage of samples, while the individual files that triggered the alerts remained.

Upon further inquiring about this event and missing files, it was later discovered that at the direction of the CEO, the archive file, named "[undisclosed].7z" was removed from storage. Based on description from the analyst working on that archive, it contained a collection of executable modules, four documents bearing classification markings, and other files related to the same project. The reason we deleted those files and will delete similar ones in the future is two-fold; We don't need anything other than malware binaries to improve protection of our customers and secondly, because of concerns regarding the handling of potential classified materials. Assuming that the markings were real, such information cannot and will not consumed even to produce detection signatures based on descriptions.

This concern was later translated into a policy for all malware analysts which are required to delete any potential classified materials that have been accidentally collected during anti-malware research or received from a third party. Again to restate: to the best of our knowledge, it appears the archive files and documents were removed from our storage, and only individual executable files (malware) that were already detected by our signatures were left in storage. Also, it is very apparent that no documents were actively "detected on" during this process. In other words, the only files that fired on specific Equation signatures were binaries, contained within an archive or outside of it. The documents were inadvertently pulled back because they were contained within the larger archive file that alerted on many Equation signatures. According to security software industry standards, requesting a copy of an archive containing malware is a legitimate request, which often helps security companies locate data containers used by malware droppers (i.e. they can be self-extracting archives or even infected ISO files).

An Interesting Twist

During the investigation, we also discovered a very interesting twist to the story that has not been discussed publicly to our knowledge. Since we were attempting to be as thorough as possible, we analyzed EVERY alert ever triggered for the specific system in question and came to a very interesting conclusion. It appears the system was actually compromised by a malicious actor on October 4, 2014 at 23:38 local time, specifically by a piece of malware hidden inside a malicious MS Office ISO, specifically the "setup.exe" file (md5: a82c0575f214bdc7c8ef5a06116cd2a4 – for detection coverage, see this VirusTotal link) .

Looking at the sequence of events and detections on this system, we quickly noticed that the user in question ran the above file with a folder name of "Office-2013-PPVL-x64-en-US-Oct2013.iso". What is interesting is that this ISO file is malicious and was mounted and subsequently installed on the system along with files such as "kms.exe" (a name of a popular pirated software activation tool), and "kms.activator.for.microsoft.windows.8.server.2012.and.office.2013.all.editions". Kaspersky Lab products detected the malware with the verdict **Backdoor.Win32.Mokes.hvl**.

At a later time after installation of the supposed MS Office 2013, the antivirus began blocking connections out on a regular basis to the URL "http://xvidmovies[.]in/dir/index.php". Looking into this domain, we can quickly find other malicious files that beacon to the same URL. It's important to note that the reason we know the system was beaconing to this URL is because we were actively blocking it as it was a known bad site. This does however indicate the user actively downloaded / installed malware on the same system around the same time frame as our detections on the Equation files.

To install and run this malware, the user must have disabled Kaspersky Lab products on his machine. Our telemetry does not allow us to say when the antivirus was disabled, however, the fact that the malware was later detected as running in the system suggests the antivirus had been disabled or was not running when the malware was run. **Executing the malware would not have been possible with the antivirus enabled**.

Additionally, there also may have been other malware from different downloads that we were unaware of during this time frame. Below is a complete list of the 121 non-Equation specific alerts seen on this system over the two month time span:

Backdoor.OSX.Getshell.k
Backdoor.Win32.Mokes.hvl
Backdoor.Win32.Shiz.gpmv
Backdoor.Win32.Swrort.dbq
DangerousObject.Multi.Chupitio.a
Exploit.Java.Agent.f
Exploit.Java.CVE-2009-3869.a
Exploit.Java.CVE-2010-0094.bb
Exploit.Java.CVE-2010-0094.e
Exploit.Java.CVE-2010-0094.q
Exploit.Java.CVE-2010-0840.gm
Exploit.Java.CVE-2010-0842.d
Exploit.Java.CVE-2010-3563.a
Exploit.Java.CVE-2011-3544.ac
Exploit.Java.CVE-2012-0507.al
Exploit.Java.CVE-2012-0507.je
Exploit.Java.CVE-2012-1723.ad
Exploit.Java.CVE-2012-4681.l
Exploit.JS.Aurora.a
Exploit.MSVisio.CVE-2011-3400.a

Exploit.Multi.CVE-2012-0754.a
Exploit.OSX.Smid.b
Exploit.SWF.CVE-2010-1297.c
Exploit.SWF.CVE-2011-0609.c
Exploit.SWF.CVE-2011-0611.ae
Exploit.SWF.CVE-2011-0611.cd
Exploit.Win32.CVE-2010-0188.a
Exploit.Win32.CVE-2010-0480.a
Exploit.Win32.CVE-2010-3653.a
Exploit.Win32.CVE-2010-3654.a
HackTool.Win32.Agent.vhs
HackTool.Win32.PWDump.a
HackTool.Win32.WinCred.e
HackTool.Win32.WinCred.i
HackTool.Win64.Agent.b
HackTool.Win64.WinCred.a
HackTool.Win64.WinCred.c
HEUR:Exploit.FreeBSD.CVE-2013-2171.a
HEUR:Exploit.Java.CVE-2012-1723.gen
HEUR:Exploit.Java.CVE-2013-0422.gen
HEUR:Exploit.Java.CVE-2013-0431.gen
HEUR:Exploit.Java.CVE-2013-2423.gen
HEUR:Exploit.Java.Generic
HEUR:Exploit.Script.Generic
HEUR:HackTool.AndroidOS.Revtcp.a
HEUR:Trojan-Downloader.Script.Generic
HEUR:Trojan-FakeAV.Win32.Onescan.gen
HEUR:Trojan.Java.Generic
HEUR:Trojan.Script.Generic
HEUR:Trojan.Win32.Generic
Hoax.Win32.ArchSMS.cbzph
KHSE:Exploit.PDF.Generic.a
not-a-virus:AdWare.JS.MultiPlug.z
not-a-virus:AdWare.NSIS.Agent.bx
not-a-virus:AdWare.Win32.Agent.allm
not-a-virus:AdWare.Win32.AirAdInstaller.cdgd
not-a-virus:AdWare.Win32.AirAdInstaller.emlr
not-a-virus:AdWare.Win32.Amonetize.fay
not-a-virus:AdWare.Win32.DomaIQ.cjw
not-a-virus:AdWare.Win32.Fiseria.t
not-a-virus:AdWare.Win32.iBryte.jda
not-a-virus:AdWare.Win32.Inffinity.yas
not-a-virus:AdWare.Win32.MultiPlug.nbjr
not-a-virus:AdWare.Win32.Shopper.adw
not-a-virus:Downloader.NSIS.Agent.am
not-a-virus:Downloader.NSIS.Agent.an

not-a-virus:Downloader.NSIS.Agent.as
not-a-virus:Downloader.NSIS.Agent.go
not-a-virus:Downloader.NSIS.Agent.lf
not-a-virus:Downloader.NSIS.OutBrowse.a
not-a-virus:Downloader.Win32.Agent.bxib
not-a-virus:Monitor.Win32.Hooker.br
not-a-virus:Monitor.Win32.KeyLogger.xh
not-a-virus:PSWTool.Win32.Cain.bp
not-a-virus:PSWTool.Win32.Cain.bq
not-a-virus:PSWTool.Win32.CredDump.a
not-a-virus:PSWTool.Win32.FirePass.ia
not-a-virus:PSWTool.Win32.NetPass.amv
not-a-virus:PSWTool.Win32.PWDump.3
not-a-virus:PSWTool.Win32.PWDump.4
not-a-virus:PSWTool.Win32.PWDump.5
not-a-virus:PSWTool.Win32.PWDump.ar
not-a-virus:PSWTool.Win32.PWDump.at
not-a-virus:PSWTool.Win32.PWDump.bey
not-a-virus:PSWTool.Win32.PWDump.bkr
not-a-virus:PSWTool.Win32.PWDump.bve
not-a-virus:PSWTool.Win32.PWDump.f
not-a-virus:PSWTool.Win32.PWDump.sa
not-a-virus:PSWTool.Win32.PWDump.yx
not-a-virus:RiskTool.Win32.WinCred.gen
not-a-virus:RiskTool.Win64.WinCred.a
not-a-virus:WebToolbar.JS.Condonit.a
not-a-virus:WebToolbar.Win32.Agent.avl
not-a-virus:WebToolbar.Win32.Cossder.updv
not-a-virus:WebToolbar.Win32.Cossder.uubg
not-a-virus:WebToolbar.Win32.MyWebSearch.sv
PDM:Trojan.Win32.Badur.a
Trojan-Banker.Win32.Agent.kan
Trojan-Downloader.Win32.Genome.jlcv
Trojan-Dropper.Win32.Injector.jqmj
Trojan-Dropper.Win32.Injector.ktep
Trojan-FakeAV.Win64.Agent.j
Trojan-Ransom.Win32.ZedoPoo.phd
Trojan.Java.Agent.at
Trojan.Win32.Adond.lbgp
Trojan.Win32.Buzus.umzt
Trojan.Win32.Buzus.uuzf
Trojan.Win32.Diple.fygv
Trojan.Win32.Genome.amqoa
Trojan.Win32.Genome.amtor
Trojan.Win32.Genome.kpzv
Trojan.Win32.Genome.ngd

Trojan.Win32.Inject.euxi
Trojan.Win32.Starter.ceg
Trojan.Win32.Swisyn.aaig
UDS:DangerousObject.Multi.Generic
UFO:(blocked)
VirTool.Win32.Rootkit
VirTool.Win32.Topo.12
Virus.Win32.Suspic.gen
WMUF:(blocked)

Conclusions

At this point, we had the answers to the questions we felt could be answered. To summarize, we will address each one below:

Q1 – Was our software used outside of its intended functionality to pull classified information from a person's computer?

A1 – The software performed as expected and notified our analysts of alerts on signatures written to detect on Equation group malware that was actively under investigation. In no way was the software used outside of this scope to either pull back additional files that did not fire on a malware signature or were not part of the archive that fired on these signatures.

Q2 – When did this incident occur?

A2 – In our professional opinion, the incident spanned between September 11, 2014 and November 17, 2014.

Q3 – Who was this person?

A3 – Because our software anonymizes certain aspects of users' information, we are unable to pinpoint specifically who the user was. Even if we could, disclosing such information is against our policies and ethical standards. What we can determine is that the user was originating from an IP address that is supposedly assigned to a Verizon FiOS address pool for the Baltimore, MD and surrounding area.

Q4 – Was there actually classified information found on the system inadvertently?

A4 – What is believed to be potentially classified information was pulled back because it was contained within an archive that fired on an Equation specific malware signatures. Besides malware, the archive also contained what appeared to be source code for Equation malware and four Word documents bearing classification markings.

Q5 – If classified information was pulled back, what happened to said data after? Was it handled appropriately?

A5 – After discovering the suspected Equation malware source code and classified documents, the analyst reported the incident to the CEO. Following a request from the CEO, the archive was deleted from all of our systems. With the archive that contained the classified information being subsequently removed from our storage locations, only traces of its detection remain in our system (i.e. – statistics and some metadata). We cannot assess whether the data was "handled appropriately" (according to US Government norms) since our analysts have not been trained on handling US classified information, nor are they under any legal obligation to do so.

Q6 – Why was the data pulled back in the first place? Is the evidence this information was passed on to "Russian Hackers" or Russian intelligence?

A6 – The information was pulled back because the archive fired on multiple Equation malware signatures. We also found no indication the information ever left our corporate networks. Transfer of a malware file is done with appropriate encryption level relying on RSA+AES with an acceptable key length, which should exclude attempts to intercept such data anywhere on the network between our security software and the analyst receiving the file.

Q7 – What types of files were gathered from the supposed system?

A7 – Based on statistics, the files that were submitted to Kaspersky Lab were mostly malware samples and suspected malicious files, either stand-alone, or inside a 7zip archive. The only files stored to date still in our sample collection from this incident are malicious binaries.

Q8 – Do we have any indication the user was subsequently "hacked" by Russian actors and data exfiltrated?

A8 – Based on the detections and alerts found in the investigation, the system was most likely compromised during this time frame by unknown threat actors. We asses this from the fact that the user installed a backdoored MS Office 2013 illegal activation tool, detected by our products as Backdoor.Win32.Mokes.hvl. To run this malware, the user must have disabled the AV protection, since running it with the antivirus enabled would not have been possible. This malicious software is a Trojan (later identified as "Smoke Bot" or "Smoke Loader") allegedly created by a Russian hacker in 2011 and made available on Russian underground forums for purchase. During the period of September 2014-November 2014, the command and control servers of this malware were registered to presumably a Chinese entity going by the name "Zhou Lou", from Hunan, using the e-mail address "zhoulu823@gmail.com". We are still working on this and further details on this malware might be made available later as a separate research paper.

Of course, the possibility exists that there may have been other malware on the system which our engines did not detect at the time of research. Given that system owner's potential clearance level, the user could have been a prime target of nation states. Adding the user's apparent need for cracked versions of Windows and Office, poor security practices, and improper handling of what appeared to be classified materials, it is possible that the user could have leaked information to many hands. What we are certain about is that any non-malware data that we received based on passive consent of the user was deleted from our storage.

Q9 – Could Kaspersky Lab products be secretly used to intentionally siphon sensitive data unrelated to malware from customers' computers?

A9 – 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. With great access comes great responsibility and that is why a procedure to create a signature that would request a file from a user's computer has to be carefully handled. Kaspersky malware analysts have rights to create signatures. Once created, these signatures are reviewed and committed by another group within Kaspersky Lab to ensure proper checks and balances. If there were an external attempt to create a signature, that creation would be visible not only in internal databases and historical records, but also via external monitoring of all our released signatures by third parties. Considering that our signatures are regularly reversed by other researchers, competitors, and offensive research companies, if any morally questionable signatures ever existed it would have already been discovered. Our internal analysis and searching revealed no such signatures as well.

In relation to Equation research specifically, our checks verified that during 2014-2016, none of the researchers working on Equation possessed the rights to commit signatures directly without having an experienced signature developer verifying those. If there was a doubtful intention in signatures during the hunt for Equation samples, this would have been questioned and reported by a lead signature developer.

Q10 – Assuming cyberspies were able to see screens of our analysts, what could they find on it and how could that be interpreted?

A10 – We have done a thorough search for keywords and classification markings in our signature databases. The result was negative: we never created any signatures on known classification markings. However, during this sweep we discovered something interesting in relation to TeamSpy research that we published earlier (for more details we recommend to check the original research at https://securelist.com/the-teamspy-crew-attacks-abusing-teamviewer-for-cyberespionage-8/35520/). TeamSpy malware was designed to automatically collect certain files that fell into the interest of the attackers. They defined a list of file extensions, such as office documents (*.doc, *.rtf, *.xls, *.mdb), pdf files (*.pdf) and more. In addition, they used wildcard string pattern based on keywords in the file names, such as *pass*, *secret*, *saidumlo* (meaning "secret" in Georgian) and others. These patterns were hardcoded into the malware that we discovered earlier, and could be used to detect similar malware samples. We did discover a signature created by a malware analyst in 2015 that was looking for the following patterns:

- *saidumlo*
- *secret*.*
- *.xls
- *.pdf
- *.pgp
- *pass*.*

These strings had to be located in the body of the malware dump from a sandbox processed sample. In addition, the malware analyst included another indicator to avoid false positives; A path where the malware dropper stored dropped files: ProgramData\Adobe\AdobeARM.

One could theorize about an intelligence operator monitoring a malware analyst's work in the process of entering these strings during the creation of a signature. We cannot say for sure, but it is a possibility that an attacker looking for anything that can expose our company from a negative side, observations like this may work as a trigger for a biased mind. Despite the intentions of the malware analyst, they could have been interpreted wrongly and used to create false allegations against us, supported by screenshots displaying these or similar strings.

Many people including security researchers, governments, and even our direct competitors from the private sector have approached us to express support. It is appalling to see that accusations against our company continue to appear without any proof or factual information being presented. Rumors, anonymous sources, and lack of hard evidence spreads only fear, uncertainty and doubt. We hope that this report sheds some long-overdue light to the public and allows people to draw their own conclusions based on the facts presented above. We are also open and willing to do more, should that be required.

Exhibit 8

Kaspersky Anti-Virus 2013

201820172016

End User License Agreement for Kaspersky Anti-Virus

Back to "Licensing and Activation"
2013 Mar 19 ID: 8752

IMPORTANT LEGAL NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT BEFORE YOU START USING THE SOFTWARE.

BY CLICKING THE ACCEPT BUTTON IN THE LICENSE AGREEMENT WINDOW OR BY ENTERING CORRESPONDING SYMBOL(-S) YOU CONSENT TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. SUCH ACTION IS A SYMBOL OF YOUR SIGNATURE AND YOU ARE CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THIS AGREEMENT AND AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU. IF YOU DO NOT AGREE TO ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT, CANCEL THE INSTALLATION OF THE SOFTWARE AND DO NOT INSTALL THE SOFTWARE.

AFTER CLICKING THE ACCEPT BUTTON IN THE LICENSE AGREEMENT WINDOW OR AFTER ENTERING CORRESPONDING SYMBOL(-S) YOU HAVE THE RIGHT TO USE THE SOFTWARE IN ACCORDANCE WITH THE TERMS AND CONDITIONS OF THIS AGREEMENT.

1. Definitions

1.1. **Software** means software including any Updates and related materials.
1.2. **Rightholder** (owner of all rights, whether exclusive or otherwise to the Software) means Kaspersky Lab ZAO, a company incorporated according to the laws of the Russian Federation.
1.3. **Computer(s)** means hardware, including personal computers, laptops, workstations, personal digital assistants, "smart phones", handheld devices, or other electronic devices for which the Software was designed where the Software will be installed and/or used.
1.4. **End User** (You/Your) means individual(s) installing or using the Software on their own behalf or who are legally using a copy of the Software; or, if the Software is being downloaded or installed on behalf of an organization, such as an employer, "You" further means the organization for which the Software is downloaded or installed and it is represented hereby that such organization has authorized the person accepting this agreement to do so on its behalf. For purposes hereof the term "organization", without limitation, includes any partnership, limited liability company, corporation, association, joint stock company, trust, joint venture, labor organization, unincorporated organization, or governmental authority.
1.5. **Partner(s)** means organizations or individual(s) who distribute the Software based on an agreement and license with the Rightholder.
1.6. **Update(s)** means all upgrades, revisions, patches, enhancements, fixes, modifications, copies, additions or maintenance packs, etc.
1.7. **User Manual** means user manual, administrator guide, reference book and related explanatory or other materials.

2. Grant of License

2.1. You are given a non-exclusive license to store, load, install, execute, and display (to "use") the Software on a specified number of Computers in order to assist in protecting Your Computer on which the Software is installed, from threats described in the User Manual, according to all technical requirements described in the User Manual and according to the terms and conditions of this Agreement (the "License") and you accept this License:
Trial Version. If you have received, downloaded and/or installed a trial version of the Software and are hereby granted an evaluation license for the Software, you may use the Software only for evaluation purposes and only during the single applicable evaluation period, unless otherwise indicated, from the date of the initial installation. Any use of the Software for other purposes or beyond the applicable evaluation period is strictly prohibited.
Multiple-Environment Software; Multiple-Language Software; Dual-Media Software; Multiple Copies; Bundles. If you use different versions of the Software or different language editions of the Software, if you receive the Software on multiple media, if you otherwise receive multiple copies of the Software, or if you received the Software bundled with other software, the total permitted number of your Computers on which all versions of the Software are installed shall correspond to the number of computers specified in licenses you have obtained from the Rightholder provided that, unless the licensing terms provide otherwise, each acquired license entitles you to install and use the Software on such number of Computer(s) as is specified in Clauses 2.2 and 2.3.
2.2. If the Software was acquired on a physical medium You have the right to use the Software for protection of such number of Computer(s) as is specified on the Software package.
2.3. If the Software was acquired via the Internet You have the right to use the Software for protection of such number of Computers as was specified when You acquired the License to the Software.

2.4. You have the right to make a copy of the Software solely for backup purposes and only to replace the legally owned copy if such copy is lost, destroyed or becomes unusable. This backup copy cannot be used for other purposes and must be destroyed when you lose the right to use the Software or when Your license expires or is terminated for any other reason according to the legislation in force in the country of your principal residence or in the country where You are using the Software.
2.5. You can transfer the non-exclusive license to use the Software to other individuals within the scope of the license granted by the Rightholder to You, provided that the recipient agrees to be bound by all the terms and conditions of this Agreement and to replace you in full in the license granted by the Rightholder. In case You fully transfer the rights granted from the Rightholder to use the Software You must destroy all copies of the Software, including the backup copy. If You are a recipient of a transferred license You must agree to abide by all the terms and conditions of this Agreement. If You do not agree to be bound by all the terms and conditions of this Agreement, You may not install and/or use the Software. You also agree as the recipient of a transferred license that You do not have any additional or better rights than those of the original End User who acquired the Software from the Rightholder.
2.6. To use the Software you may need to register in the My Kaspersky Account.
2.7. From the time of the Software activation or after license key file installation (with the exception of a trial version of the Software) You have the right to receive the following services for the defined period specified on the Software package (if the Software was acquired on a physical medium) or specified during acquisition (if the Software was acquired via the Internet):
- Updates of the Software via the Internet when and as the Rightholder publishes them on its website or through other online services. Any Updates that you may receive become part of the Software and the terms and conditions of this Agreement apply to them;
- Technical Support via the Internet and Technical Support telephone hotline;
- Access to information and auxiliary resources of the Rightholder.

3. Activation and Term
3.1. If You modify Your Computer or make changes to other vendors' software installed on it, You may be required by the Rightholder to repeat activation of the Software or license key file installation, the count of which may be limited by Rightholder.
3.2. If the Software was acquired on a physical medium, the Software can be used, upon your acceptance of this Agreement, for the period that is specified on the package commencing upon acceptance of this Agreement.
3.3. If the Software was acquired via the Internet, the Software can be used, upon your acceptance of this Agreement, for the period that was specified during acquisition.
3.4. If the Software was acquired on a physical medium intended for prolongation of the right to use previously acquired Software, You can repeat activation of the Software only if the activation code for previously acquired Software is present. In the absence of this activation code, the period of effective use of the Software will be limited according to the information specified on the Software package.
3.5. You have the right to use a trial version of the Software as provided in Clause 2.1 without any charge for the single applicable evaluation period (30 days) from the time of the Software activation according to this Agreement provided that the trial version does not entitle You to Updates and Technical support via the Internet and the Technical Support telephone hotline. If Rightholder sets another duration for the single applicable evaluation period You will be informed via notification.
3.6. Your License to Use the Software is limited to the period of time as specified in Clauses 3.2 or 3.3 (as applicable) and the remaining period can be viewed via means described in the User Manual. In the expiration period described in this clause the Software may be automatically deactivated and enter into an inactive state or continue working with limited functionality.
3.7. If You have acquired Software that is intended to be used on more than one Computer then Your License

to Use the Software is limited to the period of time starting from the date of activation of the Software or license key file installation on the first Computer.
3.8. Without prejudice to any other remedy in law or in equity that the Rightholder may have, in the event of any breach by You of any of the terms and conditions of this Agreement, the Rightholder shall at any time without notice to You be entitled to terminate this License to use the Software without refunding the purchase price or any part thereof.
3.9. You agree that in using the Software and in using any report or information derived as a result of using this Software, you will comply with all applicable international, national, state, regional and local laws and regulations, including, without limitation, privacy, copyright, export control and obscenity law.
3.10. Except as otherwise specifically provided herein, you may not transfer or assign any of the rights granted to you under this Agreement or any of your obligations pursuant hereto.
3.11. The Rightholder reserves the right to limit the possibility of activation outside the region in which the Software was acquired from the Rightholder and/or its Partners.
3.12. If You have acquired the Software with an activation code valid for the language localization of the Software of the region in which it was acquired from the Rightholder or its Partners, You cannot activate the Software by applying an activation code intended for another language localization.
3.13. In case of limitations specified in Clauses 3.11 and 3.12 information about these limitations is stated on the package and/or website of the Rightholder and/or its Partners.
3.14. To check the legitimacy of the Software use the Rightholder reserves the right to use means to verify that You have licensed copy of the Software.
The Software can transmit Rightholder license information needed to verify the legitimacy of the Software use. If the check cannot be performed for a certain period of time specified in the User Manual, the Software will work with limited functionality.

4. Technical Support
4.1. The Technical Support described in Clause 2.7 of this Agreement is provided to You when the latest Update of the Software is installed (except for a trial version of the Software) in accordance with the Technical Support rules.
Technical support service and its rules are located at: http://support.kaspersky.com.
4.2. User's Data, specified in Personal Cabinet/My Kaspersky Account, can be used by Technical Support specialists only when processing User requests.

5. Information Collection
5.1. In event of an error in the installation of Software You agree to automatically transfer information about the error code, the distribution package of the Software being used, information about the Computer, as well as data from the installer about the installation of Software.
5.2. To increase the level of operational protection You agree to automatically provide information about the checksums of files processed (MD5), information to determine the reputation of URL, statistics on usage of the Software notifications, spam statistics, information about activation and the version of the Software, information about the types of identified threats, as well as the digital certificates used and information necessary to verify their authenticity. If the Computer is equipped with TPM (Trusted Platform Module), You also agree to provide the TPM report about the Computer operating system boot process and the information necessary to verify the authenticity of the report.
5.3. In order to improve security awareness about new threats and their sources and in order to improve Your security protection level the Rightholder, with your consent that has been explicitly confirmed in the Kaspersky Security Network Data Collection Statement, is expressly entitled to receive such information. You can deactivate the Kaspersky Security Network service during installation. Also, You can activate and deactivate the Kaspersky Security Network service at any time in the Software settings window.

You further acknowledge and agree that any information gathered by Rightholder can be used to track and publish reports on security risk trends in the Rightholder's sole and exclusive discretion.
5.4. The Software does not process any personally identifiable data and does not combine the processed data with any personal information.
5.5. If you do not wish for the information collected by the Software to be sent to the Rightholder, You should not activate and/or de-activate, the Kaspersky Security Network service.

6. Limitations
6.1. You shall not emulate, clone, rent, lend, lease, sell, modify, decompile, or reverse-engineer the Software or disassemble or create derivative works based on the Software or any portion thereof with the sole exception of a non-waiverable right granted to You by applicable legislation, and you shall not otherwise reduce any part of the Software to human-readable form or transfer the licensed Software, or any subset of the licensed Software, nor permit any third party to do so, except to the extent the foregoing restriction is expressly prohibited by applicable law. Neither the Software's binary code nor source may be used or reverse-engineered to re-create the program algorithm, which is proprietary. All rights not expressly granted herein are reserved by Rightholder and/or its suppliers, as applicable. Any such unauthorized use of the Software shall result in immediate and automatic termination of this Agreement and the License granted hereunder and may result in criminal and/or civil prosecution against You.
6.2. You shall not transfer the rights to use the Software to any third party except as set forth in Clause 2.5 of this Agreement.
6.3. You shall not provide the activation code and/or license key file to third parties or allow third parties access to the activation code and/or license key, which are deemed confidential data of Rightholder and you shall exercise reasonable care in protecting the activation code and/or license key in confidence provided that you can transfer the activation code and/or license key to third parties as set forth in Clause 2.5 of this Agreement. Keep the activation code in a safe place until the expiration of the license.
6.4. You shall not rent, lease or lend the Software to any third party.
6.5. You shall not use the Software in the creation of data or software used for detection, blocking or treating threats described in the User Manual.
6.6. The Rightholder has the right to block the license to use the Software in the event You breach any of the terms and conditions of this Agreement and without any refund to You.
6.7. If You are using the trial version of the Software You do not have the right to receive the Technical Support specified in Clause 4 of this Agreement and You do not have the right to transfer the license or the rights to use the Software to any third party.

7. Limited Warranty and Disclaimer
7.1. The Rightholder guarantees that the Software will substantially perform according to the specifications and descriptions set forth in the User Manual provided however that such limited warranty shall not apply to the following: (w) Your Computer's deficiencies and related infringement for which Rightholder's expressly disclaims any warranty responsibility; (x) malfunctions, defects, or failures resulting from misuse; abuse; accident; neglect; improper installation, operation or maintenance; theft; vandalism; acts of God; acts of terrorism; power failures or surges; casualty; alteration, non-permitted modification, or repairs by any party other than Rightholder; or any other third parties' or Your actions or causes beyond Rightholder's reasonable control; (y) any defect not made known by You to Rightholder as soon as practical after the defect first appears; and (z) incompatibility caused by hardware and/or software components installed on Your Computer.
7.2. You acknowledge, accept and agree that no software is error-free and You are advised to back up the Computer with the frequency and reliability suitable for You.
7.3. The Rightholder does not provide any guarantee that the Software will work correctly in case of

violations of the terms described in the User Manual or in this Agreement.
7.4. The Rightholder does not guarantee that the Software will work correctly if You do not regularly download Updates specified in Clause 2.7 of this Agreement.
7.5. The Rightholder does not guarantee protection from the threats described in the User Manual after the expiration of the period specified in Clauses 3.2 or 3.3 of this Agreement or after the License to use the Software is terminated for any reason.
7.6. You acknowledge that the Software will be provisioned with Kaspersky standard settings applied by default and that it is Your sole responsibility to configure the Software to satisfy Your own requirements.
7.7. THE SOFTWARE IS PROVIDED "AS IS" AND THE RIGHTHOLDER MAKES NO REPRESENTATION AND GIVES NO WARRANTY AS TO ITS USE OR PERFORMANCE. EXCEPT FOR ANY WARRANTY, CONDITION, REPRESENTATION OR TERM THE EXTENT TO WHICH CANNOT BE EXCLUDED OR LIMITED BY APPLICABLE LAW. THE RIGHTHOLDER AND ITS PARTNERS MAKE NO WARRANTY, CONDITION, REPRESENTATION, OR TERM (EXPRESSED OR IMPLIED, WHETHER BY STATUTE, COMMON LAW, CUSTOM, USAGE OR OTHERWISE) AS TO ANY MATTER INCLUDING, WITHOUT LIMITATION, NON-INFRINGEMENT OF THIRD-PARTY RIGHTS, MERCHANTABILITY, SATISFACTORY QUALITY, INTEGRATION, OR APPLICABILITY FOR A PARTICULAR PURPOSE. YOU ASSUME ALL FAULTS, AND THE ENTIRE RISK AS TO PERFORMANCE AND RESPONSIBILITY FOR SELECTING THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS, AND FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE SOFTWARE. WITHOUT LIMITING THE FOREGOING PROVISIONS, THE RIGHTHOLDER MAKES NO REPRESENTATION AND GIVES NO WARRANTY THAT THE SOFTWARE WILL BE ERROR-FREE OR FREE FROM INTERRUPTIONS OR OTHER FAILURES OR THAT THE SOFTWARE WILL MEET ANY OR ALL OF YOUR REQUIREMENTS WHETHER OR NOT DISCLOSED TO THE RIGHTHOLDER.

8. Exclusion and Limitation of Liability
8.1. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE RIGHTHOLDER OR ITS PARTNERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR LOSS OF PRIVACY, FOR CORRUPTION, DAMAGE AND LOSS OF DATA OR PROGRAMS, FOR FAILURE TO MEET ANY DUTY INCLUDING ANY STATUTORY DUTY, DUTY OF GOOD FAITH OR DUTY OF REASONABLE CARE, FOR NEGLIGENCE, FOR ECONOMIC LOSS, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER SERVICES, INFORMATION, SOFTWARE, AND RELATED CONTENT THROUGH THE SOFTWARE OR OTHERWISE ARISING OUT OF THE USE OF THE SOFTWARE, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS AGREEMENT, OR ARISING OUT OF ANY BREACH OF CONTRACT OR ANY TORT (INCLUDING NEGLIGENCE, MISREPRESENTATION, ANY STRICT LIABILITY OBLIGATION OR DUTY), OR ANY BREACH OF STATUTORY DUTY, OR ANY BREACH OF WARRANTY OF THE RIGHTHOLDER OR ANY OF ITS PARTNERS, EVEN IF THE RIGHTHOLDER OR ANY PARTNER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

YOU AGREE THAT IN THE EVENT THE RIGHTHOLDER AND/OR ITS PARTNERS ARE FOUND LIABLE, THE LIABILITY OF THE RIGHTHOLDER AND/OR ITS PARTNERS SHALL BE LIMITED BY THE COSTS OF THE SOFTWARE. IN NO CASE SHALL THE LIABILITY OF THE

RIGHTHOLDER AND/OR ITS PARTNERS EXCEED THE FEES PAID FOR THE SOFTWARE TO THE RIGHTHOLDER OR THE PARTNER (AS MAY BE APPLICABLE).

NOTHING IN THIS AGREEMENT EXCLUDES OR LIMITS ANY CLAIM FOR DEATH AND PERSONAL INJURY. FURTHER IN THE EVENT ANY DISCLAIMER, EXCLUSION OR LIMITATION IN THIS AGREEMENT CANNOT BE EXCLUDED OR LIMITED ACCORDING TO APPLICABLE LAW THEN ONLY SUCH DISCLAIMER, EXCLUSION OR LIMITATION SHALL NOT APPLY TO YOU AND YOU CONTINUE TO BE BOUND BY ALL THE REMAINING DISCLAIMERS, EXCLUSIONS AND LIMITATIONS.

9. GNU and Other Third-Party Licenses

9.1. The Software may include some software programs that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar free software licenses which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code "Open-Source Software"). If such licenses require that for any software, which is distributed to someone in an executable binary format, that the source code also be made available to those users, then the source code should be made available by sending the request to source@kaspersky.com or the source code is supplied with the Software. If any Open-Source Software licenses require that the Rightholder provide rights to use, copy or modify an Open-Source Software program that are broader than the rights granted in this Agreement, then such rights shall take precedence over the rights and restrictions herein.

10. Intellectual Property Ownership

10.1. You agree that the Software and the authorship, systems, ideas, methods of operation, documentation and other information contained in the Software are proprietary intellectual property and/or the valuable trade secrets of the Rightholder or its partners and that the Rightholder and its partners, as applicable, are protected by civil and criminal law, and by the law of copyright, trade secret, trademark and patent of the Russian Federation, European Union and the United States, as well as other countries and international treaties. This Agreement does not grant You any rights to the intellectual property, including any Trademarks or Service Marks of the Rightholder and/or its partners ("Trademarks"). You may use the Trademarks only insofar as to identify printed output produced by the Software in accordance with accepted trademark practice, including identification of the Trademark owner’s name. Such use of any Trademark does not give you any rights of ownership in that Trademark. The Rightholder and/or its partners own and retain all right, title, and interest in and to the Software, including without limitation any error corrections, enhancements, Updates or other modifications to the Software, whether made by the Rightholder or any third party, and all copyrights, patents, trade secret rights, trademarks, and other intellectual property rights therein. Your possession, installation or use of the Software does not transfer to you any title to the intellectual property in the Software, and you will not acquire any rights to the Software except as expressly set forth in this Agreement. All copies of the Software made hereunder must contain the same proprietary notices that appear on and in the Software. Except as stated herein, this Agreement does not grant you any intellectual property rights in the Software and you acknowledge that the License, as further defined herein, granted under this Agreement only provides you with a right of limited use under the terms and conditions of this Agreement. Rightholder reserves all rights not expressly granted to you in this Agreement.

10.2. You agree not to modify or alter the Software in any way. You may not remove or alter any copyright notices or other proprietary notices on any copies of the Software.

11. Governing Law

11.1. Except as provided in Clauses 11.2 and 11.3 below, this Agreement shall be governed by and construed in accordance the laws specified below for the country or territory in which you obtained the Software,

without reference to or application of conflicts of laws
principles:
a. Russia. If you obtained the Software in Russia, the laws of the Russian Federation.
b. United States, Puerto Rico, American Samoa, Guam, and U.S. Virginia Islands. If you obtained the Software in the United States, Puerto Rico,
American Samoa, Guam or the U.S. Virgin Islands, the laws of the State of Massachusetts, USA, provided, however, that the laws of the U.S. state where you live will govern claims under state consumer protection, unfair competition, or similar laws. To the fullest extent permitted by law, the Rightholder and you expressly agree hereby to waive any right to a trial by jury.
c. Canada. If you obtained the Software in Canada, the laws of the Province of Ontario.
d. Mexico. If you obtained the Software in Mexico, the federal laws of the Republic of Mexico.
e. European Union (EU). If you obtained the Software in a member country of the EU, the laws of England.
f. Australia. If you obtained the Software in Australia, the laws of the State or Territory in which you obtained the license.
g. Hong Kong Special Administration Region (SAR) and Macau SAR. If you obtained the Software in Hong Kong SAR or Macau SAR, the laws
of Hong Kong SAR.
h. Taiwan. If you obtained the Software in Taiwan, the laws of Taiwan.
i. Japan. If you obtained the Software in Japan, the laws of Japan.
j. Any Other Country or Territory. If you obtained the Software in any other country, the substantive laws of the country where the purchase took place would be in effect.
11.2. Notwithstanding the foregoing, if the mandatory laws or public policy of any country or territory in which this Agreement is enforced or construed prohibit the application of the law specified herein, then the laws of such country or territory shall instead apply to the extent required by such mandatory laws or public policy. Similarly, if you are an individual consumer, the provisions of Clause 11.1 shall not affect any mandatory right you may have to take action in your country of residence under the laws of that country.
11.3. This Agreement shall not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded.

12. Period for Bringing Actions
12.1. No action, regardless of form, arising out of the transactions under this Agreement may be brought by either party hereto more than one (1) year after the cause of action has occurred, or was discovered to have occurred, except that an action for infringement of intellectual property rights may be brought within the maximum applicable statutory period.

13. Entire Agreement; Severability; No Waiver
13.1. This Agreement is the entire agreement between you and Rightholder and supersedes any other prior agreements, proposals, communications or advertising, oral or written, with respect to the Software or to the subject matter of this Agreement. You acknowledge that you have read this Agreement, understand it and agree to be bound by its terms. If any provision of this Agreement is found by a court of competent jurisdiction to be invalid, void, or unenforceable for any reason, in whole or in part, such provision will be more narrowly construed so that it becomes legal and enforceable, and the entire Agreement will not fail on account thereof and the balance of the Agreement will continue in full force and effect to the maximum extent permitted by law or equity while preserving, to the fullest extent possible, its original intent. No waiver of any provision or condition herein shall be valid unless in writing and signed by you and an authorized representative of Rightholder provided that no waiver of any breach of any provisions of this Agreement will constitute a waiver of any prior, concurrent or subsequent breach. Rightholder’s failure to insist upon or enforce strict performance of any provision of this Agreement or any right shall not be construed as a waiver

of any such provision or right.

14. Rightholder Contact Information

Should you have any questions concerning this Agreement, or if you desire to contact the Rightholder for any reason, please contact our Customer Service Department at:

Kaspersky Lab ZAO, 10 build. 1, 1st Volokolamsky Proezd
Moscow, 123060 Russian Federation
E-mail: info@kaspersky.com
Web site: www.kaspersky.com

Back to "Licensing and Activation"

Support for Home

Consumer Support Contacts
Contact support via My Kaspersky
Knowledge Base for Home
How-to Videos
Forum

Virus-fighting tools & services

Scan file or URL for viruses
Report a false alarm
Kaspersky Virus Removal Tool
Kaspersky Rescue Disk
Other virus-fighting tools

Support for Small Business

Small Business Support Contacts
Contact support via My Kaspersky
Knowledge Base for Small Business
Forum

Software Downloads

Buy online
Renew license
Get updates
Free trial download

Support terms and conditions
(updated April 12, 2017)

Support for Business

Business Support Contacts
Contact support via CompanyAccount
Knowledge Base for Business
Product Support Lifecycle
Premium Support Plans
Licensing by Subscription
Forum
Online Trainings
Subscribe to news

Site Feedback

-
-
-
-
-
-

Have you found what you were looking for?

Please let us know how we can make this website more comfortable for you

```
Enter your feedback
here (max. 500
```

Send feedback Send feedback

Thank you!

Thank you for submitting your feedback.
We will review your feedback shortly.

Exhibit 9

Kaspersky Anti-Virus 2018

201820172016

End User License Agreement for Kaspersky Anti-Virus 2018

Back to "Licensing and Activation"
2017 Aug 21 ID: 13596

END USER LICENSE AGREEMENT

IMPORTANT LEGAL NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT BEFORE YOU START USING THE SOFTWARE.

Running the Software, clicking the button that confirms that You accept the License Agreement during installation, or entering the corresponding character(s), constitutes Your unconditional acceptance of the terms of this License Agreement. If You do not agree with the terms of this License Agreement, You must abort the installation of the Software and\or delete the Software.

AFTER CLICKING THE BUTTON, THAT CONFIRMS YOUR ACCEPTANCE IN THE LICENSE AGREEMENT WINDOW OR AFTER ENTERING CORRESPONDING SYMBOL(S), YOU HAVE THE RIGHT TO USE THE SOFTWARE IN ACCORDANCE WITH THE TERMS AND CONDITIONS OF THIS AGREEMENT.

IF THERE IS A LICENSE CONTRACT IN ITS WRITTEN FORM OR A LICENSE CERTIFICATE ACCOMPANYING THE SOFTWARE, THE TERMS OF THE SOFTWARE USE DEFINED IN THE LICENSE CONTRACT OR LICENSE CERTIFICATE PREVAILS OVER THE CURRENT END USER LICENSE AGREEMENT.

1. Definitions
1.1. Software means software including any Updates and related materials.
1.2. Rightholder (owner of all rights, whether exclusive or otherwise to the Software) means AO Kaspersky Lab, a company incorporated according to the laws of the Russian Federation.
1.3. Computer — the operating system, virtual machine or hardware, including the workstation, mobile device or server for which the Software is intended and/or on which the Software is to be installed and/or used.
1.4. End User (You/Your) means individual(s) installing or using the Software on their own behalf or who are legally using a copy of the Software; or, if the Software is being downloaded or installed on behalf of an organization, such as an employer, "You" further means the organization for which the Software is downloaded or installed and it is represented hereby that this organization has authorized the person accepting this agreement to do so on its behalf. For purposes hereof the term "organization", without limitation, includes any partnership, limited liability company, corporation, association, joint stock company, trust, joint venture, labor organization, unincorporated organization, or governmental authority. For Software distributed free of charge, excluding Software provided for evaluation purposes, End User (You/Your) means only individual(s).
1.5. Partner(s) means organizations or individual(s) who distribute the Software based on an agreement and license with the Rightholder.
1.6. Update(s) — anti-virus databases, improvements, patches, expansions and/or modifications for the Software.
1.7. Software expansions — additional software components and services provided by the Rightholder that extend the functionality of the Software and can be used with the Software or independently of it and for which a new license may need to be acquired or the existing one extended. Some expansions are provided free of charge and others for a fee. You can find out more about these expansions before acquiring them.
1.8. User Manual means user manual, administrator guide, reference book and related explanatory or other materials.
1.9. License Certificate means a document that is given to the User which is accompanied by an activation code as well as further information about the license.
1.10. The Web-Portal means the Rightholder's web resource intended to manage the installed Software and the licenses acquired.
1.11. User Account means the personal section of the Web-Portal created using data provided by the User when registering at the Web-Portal. The User Account allows the User to gain access to the Web-Portal to carry out the actions listed under pt. 1.10.
2. Grant of License
2.1. You are granted a non-exclusive license to use the Software within the scope of the functionality described in the User Manual or on the Rightholder’s Technical Support website, provided You comply with all technical requirements, restrictions and terms of use specified in this License Agreement.
Trial Version. If you have received, downloaded and/or installed a trial version of the Software and are hereby granted an evaluation license for the Software, you may use the Software only for evaluation purposes and only during the single applicable evaluation period, unless otherwise indicated, from the date of the initial installation. Any use of the Software for other purposes or beyond the applicable evaluation period is strictly prohibited.
Multiple-Environment Software; Multiple-Language Software; Dual-Media Software; Multiple Copies;

Bundles. If you use different versions of the Software or different language editions of the Software, if you receive the Software on multiple media, if you otherwise receive multiple copies of the Software, or if you received the Software bundled with other software, the total permitted number of your Computers on which all versions of the Software are installed shall correspond to the number of computers specified in licenses you have obtained from the Rightholder provided that, unless the licensing terms provide otherwise, each acquired license entitles you to install and use the Software on the number of Computer(s) and/or for the number of User Accounts as is specified in Sections 2.2 and 2.3.
The right to use the Software distributed free of charge is granted only to individuals, excluding Software provided for evaluation purposes. Software may be used by individuals only for personal non-commercial use. Use of Software distributed free of charge by legal entities excluding Software provided for evaluation purposes is strictly prohibited.
2.2. If the Software was acquired on a physical medium You have the right to use the Software for the number of Computer(s) and/or User Accounts as is specified on the Software package.
2.3. If the Software was received/acquired via the Internet You have the right to use the Software for the number of Computers and/or User Accounts as was specified when You acquired the License to the Software.
2.4. You have the right to make a copy of the Software solely for backup purposes and only to replace the legally owned copy if this copy is lost, destroyed or becomes unusable. This backup copy cannot be used for other purposes and must be destroyed when you lose the right to use the Software or when Your license expires or is terminated for any other reason according to the legislation in force in the country of your principal residence or in the country where You are using the Software.
2.5. You can transfer the non-exclusive license to use the Software to other individuals within the scope of the license granted by the Rightholder to You, provided that the recipient agrees to be bound by all the terms and conditions of this Agreement and to replace you in full in the license granted by the Rightholder. In case You fully transfer the rights granted from the Rightholder to use the Software You must destroy all copies of the Software, including the backup copy. If You are a recipient of a transferred license You must agree to abide by all the terms and conditions of this Agreement. If You do not agree to be bound by all the terms and conditions of this Agreement, You may not install and/or use the Software. You also agree as the recipient of a transferred license that You do not have any additional or better rights than those of the original End User who acquired the Software from the Rightholder.
2.6. After activating the Software within the period specified on the package (if the Software was acquired on a physical medium) or specified during purchase (if the Software acquired online), You may receive automatic Updates and the latest versions of the Software from the Rightholder or its Partners, as well as technical support according to Clause 5.
2.7. To use the Software you may need to connect the Software to the Web-Portal using Your User Account.
3. Activation and Term
3.1. If You modify Your Computer or make changes to other vendors' software installed on it, You may be required by the Rightholder to repeat activation of the Software, the count of which may be limited by the Rightholder.
3.2. If the Software was acquired on a physical medium, the Software can be used, upon your acceptance of this Agreement, for the period that is specified on the package commencing upon acceptance of this Agreement.
3.3. If the Software was received/acquired via the Internet, the Software can be used, upon your acceptance of this Agreement, for the period that was specified during acquisition.
3.4. If you have received the Software from a Partner, the period of effective use of the Software may be agreed upon between you and the Partner.
3.5. Where there is a License Certificate, the period of use of the Software is specified in the License Certificate.
3.6. Where there is a subscription, the period of use of the Software is specified when confirming the

subscription.
3.7. If the Software is activated with a free license, the period of Software usage is restricted to 1 (one) year. If the Rightholder specifies a different license period, the User is duly informed.
At the end of the period, the Rightholder may provide a new limited free license to use the Software. In this case, the Software is activated automatically.
3.8. If You received the Software from the Rightholder for evaluation purposes, the period of use of the Software is indicated in the relevant section of the Rightholder's website.
3.9. If the Software acquired was intended for the prolongation of the right to use previously acquired Software, You can repeat activation of the Software only if the activation code for previously acquired Software is present. In the absence of this activation code, the period of effective use of the Software will be limited according to the information specified on the Software package.
3.10. For Software activated with a license for evaluation purposes as specified in section 2.1, information about the period of use of the Software can be obtained using the methods described in the User Manual.
3.11. After expiration of the Software license, You may be entitled to continue use of the Software for a defined period of time, while the functionality of the Software may be limited. Details are available at help.kaspersky.com.
3.12. If You purchased the Software for use on more than one computer, the license period of the Software begins from the date of activation of the first Computer, or is specified in the License Certificate where such a License Certificate exists.
3.13. For the some types and versions of the Software the Rightholder enables migration away from the Software to other applications of the Rightholder. The duration of the license granted and the number of Computers after migration may be changed according to the applicable Rightholder rules. Once transition between Software has been completed, it is impossible to return to the previous Software with the current license provisions.
Important: Please read the rules governing the transition to use of other software that is available at: www.kaspersky.com/flexible_licensing.
3.14. Without prejudice to any other remedy in law or in equity that the Rightholder may have, in the event of any breach by You of any of the terms and conditions of this Agreement, the Rightholder shall at any time without notice to You be entitled to terminate this License to use the Software without refunding the purchase price or any part thereof.
3.15. The Rightholder reserves the right to limit the ability to activate the Software to the region in which the Software was intended to be sold from the Rightholder or its Partners. Information about these restrictions is available after completing the purchase of the Software license.
3.16. If You have acquired the Software with an activation code valid for the language localization of the Software of the region in which it was acquired from the Rightholder or its Partners, You cannot activate the Software by applying an activation code intended for another language localization.
3.17. In case of limitations specified in Clauses 3.15 and 3.16 information about these limitations is stated on the package and/or website of the Rightholder and/or its Partners.
3.18. To check the legitimacy of the Software's use the Rightholder reserves the right to use means to verify that You have a licensed copy of the Software.
The Software can transmit Rightholder license information needed to verify the legitimacy of the Software use.
If the check cannot be performed in a reasonable amount of time, the functionality of the Software may be limited.
4. Software components that use geolocation, the camera or GPS functions, as well as other components that supply data from the Computer or interact with My Kaspersky
4.1. You agree that use of the Software must be in accordance with its intended purpose and must not violate local legislation.

4.2. Your email address and other data provided during the account registration process can be transferred and further processed by a trusted third-party service provider of the Rightholder. This third-party service provider can process the data in countries where the level of personal data protection is lower than in Your country of residence.
4.3. You are responsible for any actions performed using Your account involving the resources of the Rightholder and/or its Partners. You agree that the Rightholder shall not be liable for the unauthorized use of Your account.
5. Technical Support
5.1. The Technical Support is provided to You in accordance with Technical Support rules.
Technical support service and its rules are located at: support.kaspersky.com.
5.2. User data stored on the Rightholder's and/or its Partner's resources may be used by Technical Support only when processing a request from the User.
6. Provision of information (if applicable)
6.1. In order to enhance the protection of information and improve the quality of the Software and services, You agree to automatically provide Kaspersky Lab with the following information of a statistical and administrative nature: information about installed programs, license data, information on detected threats and infections, checksums of processed objects, technical information about the Computer and devices connected to it, information about online activity of the device as well as You agree that such information can be provided to third-party service providers. More information is available at help.kaspersky.com.
6.2. 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.
Also, You can activate and deactivate the Kaspersky Security Network service at any time in the Software settings window.
You further acknowledge and agree that any information gathered by Rightholder can be used to track and publish reports on security risk trends at the Rightholder's sole and exclusive discretion.
If you do not wish to provide information to the Kaspersky Security Network service, You should not activate the Kaspersky Security Network service. If service is already activated, you should immediately de-activate the Kaspersky Security Network service.
Kaspersky Lab protects the information received in accordance with applicable governing law and Kaspersky Lab's rules.
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.
7. Use of the functionality of third-party online services (if applicable)
7.1. If You use Software functions linked to data storage and\or backup on third-party FTP servers or through third-party online data storage services, You must be aware that the Rightholder is not responsible for the security (confidentiality, integrity, accessibility) of data stored on these resources. Access to information and its protection is governed by the relevant terms of use of the services.
You should familiarize yourself with the terms of security for FTP servers or online services before using them.
8. Receiving informational and advertising materials
8.1. You acknowledge, accept and agree to receive informational materials via the Software from the Rightholders and/or Partners to improve the protection level.
9. Using the Adaptive Security feature
9.1. If You decide to use the Adaptive Security feature, You agree to automatically provide the information needed to generate recommendations to improve security. These recommendations will be shown in the

Web-Portal in the User Account, to which the Software is connected. Information about the recommendations shown may be used by Technical Support only when processing a request from the User.

10. Limitations

10.1. You shall not emulate, clone, rent, lend, lease, sell, modify, decompile, or reverse-engineer the Software or disassemble or create derivative works based on the Software or any portion thereof with the sole exception of a non-waiverable right granted to You by applicable legislation, and you shall not otherwise reduce any part of the Software to human-readable form or transfer the licensed Software, or any subset of the licensed Software, nor permit any third party to do so, except to the extent the foregoing restriction is expressly prohibited by applicable law. Neither the Software's binary code nor source may be used or reverse-engineered to re-create the program algorithm, which is proprietary. All rights not expressly granted herein are reserved by Rightholder and/or its suppliers, as applicable. Any unauthorized use of the Software shall result in immediate and automatic termination of this Agreement and the License granted hereunder and may result in criminal and/or civil prosecution against You.

10.2. You shall not transfer the rights to use the Software to any third party except as set forth in Section 2.5 of this Agreement.

10.3. You shall not provide the activation code to third parties or allow third parties access to the activation code and/or license key, which are deemed the confidential data of the Rightholder and you shall exercise reasonable care in protecting the activation code in confidence provided that you can transfer the activation code and/or license key to third parties as set forth in Section 2.5 of this Agreement. You are responsible for the keeping Your activation code confidential during use of the Software.

10.4. You shall not rent, lease or lend the Software to any third party.

10.5. You shall not use the Software in the creation of data or software used for detection, blocking or treating threats described in the User Manual.

10.6. If You are using the trial version of the Software You do not have the right to transfer the license or the rights to use the Software to any third party.

10.7. Violation of the intellectual rights to the Software shall result in civil, administrative or criminal liability in accordance with the law.

11. Limited Warranty and Disclaimer

11.1. The Rightholder guarantees the operation of the Software as described in the User Manual and, if supported versions of the Software are used, the installation by the User of all the latest updates for the Software, unless otherwise stipulated in the License Agreement. The list of supported versions is available at support.kaspersky.com.

11.2. You agree that the Software is supplied with the option of automatic renewal, which provides automatic downloading and installation of enhancements, patches and/or modifications for the Software and components, as well as new versions of the Software.

11.3. You agree that if needed the Software automatically downloads extensions for web browsers, which are necessary to ensure basic functionality of the licensed Software.

11.4. You acknowledge, accept and agree that no software is error-free and You are advised to back up the Computer with the frequency and reliability suitable for You.

11.5. The Rightholder does not provide any guarantee that the Software will work correctly in case of violations of the terms described in the User Manual or in this Agreement.

11.6. The Rightholder does not guarantee that the Software will work correctly if You do not regularly download Updates specified in Section 2.6 of this Agreement.

11.7. The Rightholder does not guarantee the availability of the functionality described in the User Manual on expiry of the period specified in Section 3 of this License Agreement.

11.8. You acknowledge that the Software will be provisioned with Kaspersky standard settings applied by default and that it is Your sole responsibility to configure the Software to satisfy Your own requirements.

11.9. You acknowledge and agree that the Software will engage in actions necessary for performance.

11.10. THE SOFTWARE IS PROVIDED "AS IS" AND THE RIGHTHOLDER MAKES NO REPRESENTATION AND GIVES NO WARRANTY AS TO ITS USE OR PERFORMANCE. EXCEPT FOR ANY WARRANTY, CONDITION, REPRESENTATION OR TERM THE EXTENT TO WHICH CANNOT BE EXCLUDED OR LIMITED BY APPLICABLE LAW. THE RIGHTHOLDER AND ITS PARTNERS MAKE NO WARRANTY, CONDITION, REPRESENTATION, OR TERM (EXPRESSED OR IMPLIED, WHETHER BY STATUTE, COMMON LAW, CUSTOM, USAGE OR OTHERWISE) AS TO ANY MATTER INCLUDING, WITHOUT LIMITATION, NON-INFRINGEMENT OF THIRD-PARTY RIGHTS, MERCHANTABILITY, SATISFACTORY QUALITY, INTEGRATION, OR APPLICABILITY FOR A PARTICULAR PURPOSE. YOU ASSUME ALL FAULTS, AND THE ENTIRE RISK AS TO PERFORMANCE AND RESPONSIBILITY FOR SELECTING THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS, AND FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE SOFTWARE. WITHOUT LIMITING THE FOREGOING PROVISIONS, THE RIGHTHOLDER MAKES NO REPRESENTATION AND GIVES NO WARRANTY THAT THE SOFTWARE WILL BE ERROR-FREE OR FREE FROM INTERRUPTIONS OR OTHER FAILURES OR THAT THE SOFTWARE WILL MEET ANY OR ALL OF YOUR REQUIREMENTS WHETHER OR NOT DISCLOSED TO THE RIGHTHOLDER.

12. Exclusion and Limitation of Liability

12.1. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE RIGHTHOLDER OR ITS PARTNERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR LOSS OF PRIVACY, FOR CORRUPTION, DAMAGE AND LOSS OF DATA OR PROGRAMS, FOR FAILURE TO MEET ANY DUTY INCLUDING ANY STATUTORY DUTY, DUTY OF GOOD FAITH OR DUTY OF REASONABLE CARE, FOR NEGLIGENCE, FOR ECONOMIC LOSS, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER SERVICES, INFORMATION, SOFTWARE, AND RELATED CONTENT THROUGH THE SOFTWARE OR OTHERWISE ARISING OUT OF THE USE OF THE SOFTWARE, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS AGREEMENT, OR ARISING OUT OF ANY BREACH OF CONTRACT OR ANY TORT (INCLUDING NEGLIGENCE, MISREPRESENTATION, ANY STRICT LIABILITY OBLIGATION OR DUTY), OR ANY BREACH OF STATUTORY DUTY, OR ANY BREACH OF WARRANTY OF THE RIGHTHOLDER OR ANY OF ITS PARTNERS, EVEN IF THE RIGHTHOLDER OR ANY PARTNER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

YOU AGREE THAT IN THE EVENT THE RIGHTHOLDER AND/OR ITS PARTNERS ARE FOUND LIABLE, THE LIABILITY OF THE RIGHTHOLDER AND/OR ITS PARTNERS SHALL BE LIMITED BY THE COSTS OF THE SOFTWARE. IN NO CASE SHALL THE LIABILITY OF THE RIGHTHOLDER AND/OR ITS PARTNERS EXCEED THE FEES PAID FOR THE SOFTWARE TO THE RIGHTHOLDER OR THE PARTNER (AS MAY BE APPLICABLE).

NOTHING IN THIS AGREEMENT EXCLUDES OR LIMITS ANY CLAIM FOR DEATH AND PERSONAL INJURY. FURTHER IN THE EVENT ANY DISCLAIMER, EXCLUSION OR LIMITATION IN THIS AGREEMENT CANNOT BE EXCLUDED OR LIMITED ACCORDING TO APPLICABLE LAW THEN ONLY THAT DISCLAIMER, EXCLUSION OR LIMITATION SHALL NOT APPLY TO YOU AND YOU CONTINUE TO BE BOUND BY ALL THE REMAINING DISCLAIMERS, EXCLUSIONS AND LIMITATIONS.

13. Exclusion of unlawful use

13.1. If VPN Software is available, You are entitled to use the VPN Software solely for lawful purposes.

Including, but not limited to the following, you are not entitled to use the VPN Software
-in any way that breaches any applicable local, national or international law or regulation according to the law in the country where the VPN server is located and/or were the VPN Software is used;
-for the purpose of harming or attempting to harm minors in any way;
-for the purpose of misusing the VPN Software by knowingly introducing inter alia viruses, trojans, worms, logic bombs or any other material which is malicious and/or technologically harmful;
-for the purpose of reverse engineering, decompiling, disassembling, modifying, translating, making any attempt to discover the source code of the VPN Software or creating derivative works from the VPN Software;
-for the purpose of attempting to gain unauthorized access to, interfere with, damage or disrupt the VPN Software and/or the VPN Service. We will report any such breach to the relevant law enforcement authorities and we will co-operate with those authorities by disclosing your identity to them. In the event of such a breach your right to use the VPN Software and/or the VPN Service will cease immediately;
-for the purpose of uploading, posting, emailing or otherwise transmitting any content that is directed to inciting or producing imminent conduct that is unlawful, harmful, threatening, abusive, harassing, tortuous, defamatory, vulgar, obscene, libelous, invasive of another´s privacy, hateful, or racially, ethnically or otherwise objectionable and is likely to produce such conduct;
-for the purpose of impersonating any person or entity or otherwise misrepresenting your affiliation with a person or entity;
-for the purpose of forging headers or otherwise manipulating identifiers in order to disguise the origin of any content transmitted through the VPN system;
-for the purpose of uploading, posting, emailing or otherwise transmitting any content that infringes any patent, trademark, trade secret, copyright or other intellectual property of any party;
-for the purpose of uploading, posting, emailing or otherwise transmitting any unsolicited or unauthorized advertising, promotional materials, e. g. “junk mail”, “spam”, “chain letters”, or “pyramid schemes”;
-for the purpose of interfering with or disrupting the VPN systems and/or the VPN servers and/or the VPN networks, or disobeying any requirements, procedures, policies or regulations of networks connected to our VPN systems;
-for the purpose of collecting or storing personal data about other users without their knowledge;
-for the purpose of promoting or providing instructional information about illegal activities, promoting physical harm or injury against any group or individual, or promoting any act of cruelty to animals.

14. GNU and Other Third-Party Licenses

14.1. The Software may include some software programs that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar free software licenses which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code "Open-Source Software"). If these licenses require that for any software, which is distributed to someone in an executable binary format, that the source code also be made available to those users, then the source code could be found either supplied with the Software, or could be made available by sending a request to source@kaspersky.com. If any Open-Source Software licenses require that the Rightholder provide rights to use, copy or modify an Open-Source Software program that are broader than the rights granted in this Agreement, then these rights shall take precedence over the rights and restrictions herein.

15. Intellectual Property Ownership

15.1. You agree that the Software and the authorship, systems, ideas, methods of operation, documentation and other information contained in the Software are proprietary intellectual property and/or the valuable trade secrets of the Rightholder or its partners and that the Rightholder and its partners, as applicable, are protected by civil and criminal law, and by the law of copyright, trade secret, trademark and patents of the Russian Federation, European Union and the United States, as well as other countries and international treaties. This Agreement does not grant You any rights to the intellectual property, including any Trademarks or Service

Marks of the Rightholder and/or its partners ("Trademarks"). You may use the Trademarks only insofar as to identify printed output produced by the Software in accordance with accepted trademark practice, including identification of the Trademark owner's name. Such use of any Trademark does not give you any rights of ownership in that Trademark. The Rightholder and/or its partners own and retain all right, title, and interest in and to the Software, including without limitation any error corrections, enhancements, Updates or other modifications to the Software, whether made by the Rightholder or any third party, and all copyrights, patents, trade secret rights, trademarks, and other intellectual property rights therein. Your possession, installation or use of the Software does not transfer to you any title to the intellectual property in the Software, and you will not acquire any rights to the Software except as expressly set forth in this Agreement. All copies of the Software made hereunder must contain the same proprietary notices that appear on and in the Software. Except as stated herein, this Agreement does not grant you any intellectual property rights in the Software and you acknowledge that the License, as further defined herein, granted under this Agreement only provides you with a right of limited use under the terms and conditions of this Agreement. Rightholder reserves all rights not expressly granted to you in this Agreement.

15.2. You agree not to modify or alter the Software in any way. You may not remove or alter any copyright notices or other proprietary notices on any copies of the Software.

16. Governing Law

16.1. Except as provided in Sections 16.2 and 16.3 below, this Agreement shall be governed by and construed in accordance the laws specified below for the country or territory in which you obtained the Software, without reference to or application of conflicts of laws principles:

a. Russia. If you obtained the Software in Russia, the laws of the Russian Federation.

b. United States, Puerto Rico, American Samoa, Guam, and U.S. Virgin Islands. If you obtained the Software in the United States, Puerto Rico, American Samoa, Guam or the U.S. Virgin Islands, the laws of the Commonwealth of Massachusetts, USA, provided, however, that the laws of the U.S. state where you live will govern claims under state consumer protection, unfair competition, or similar laws. To the fullest extent permitted by law, the Rightholder and you expressly agree hereby to waive any right to a trial by jury.

c. Canada. If you obtained the Software in Canada, the laws of the Province of Ontario.

d. Mexico. If you obtained the Software in Mexico, the federal laws of the Republic of Mexico.

e. European Union (EU). If you obtained the Software in a member country of the EU, the laws of England.

f. Australia. If you obtained the Software in Australia, the laws of the State or Territory in which you obtained the license.

g. Hong Kong Special Administrative Region (SAR) and Macau SAR. If you obtained the Software in Hong Kong SAR or Macau SAR, the laws of Hong Kong SAR.

h. Taiwan. If you obtained the Software in Taiwan, the laws of Taiwan.

i. Japan. If you obtained the Software in Japan, the laws of Japan.

j. Any Other Country or Territory. If you choose to obtain the Software in another country, the substantive laws of the country where the purchase took place will be in effect.

16.2. Notwithstanding the foregoing, if the mandatory laws or public policy of any country or territory in which this Agreement is enforced or construed prohibit the application of the law specified herein, then the laws of such country or territory shall instead apply to the extent required by such mandatory laws or public policy. Similarly, if you are an individual consumer, the provisions of Section 16.1 shall not affect any mandatory right you may have to take action in your country of residence under the laws of that country.

16.3. This Agreement shall not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded.

16.4. The End User is responsible for contacting only the Right Holder or their partners directly if having any problems with the product.

17. Period for Bringing Actions

17.1. No action, regardless of form, arising out of the transactions under this Agreement may be brought by

either party hereto more than one (1) year after the cause of action has occurred, or was discovered to have occurred, except that an action for infringement of intellectual property rights may be brought within the maximum applicable statutory period.

18. Entire Agreement; Severability; No Waiver

18.1. This Agreement is the entire agreement between you and Rightholder and supersedes any other prior agreements, proposals, communications or advertising, oral or written, with respect to the Software or to the subject matter of this Agreement. You acknowledge that you have read this Agreement, understand it and agree to be bound by its terms. If any provision of this Agreement is found by a court of competent jurisdiction to be invalid, void, or unenforceable for any reason, in whole or in part, such provision will be more narrowly construed so that it becomes legal and enforceable, and the entire Agreement will not fail on account thereof and the balance of the Agreement will continue in full force and effect to the maximum extent permitted by law or equity while preserving, to the fullest extent possible, its original intent. No waiver of any provision or condition herein shall be valid unless in writing and signed by you and an authorized representative of Rightholder provided that no waiver of any breach of any provisions of this Agreement will constitute a waiver of any prior, concurrent or subsequent breach. Rightholder’s failure to insist upon or enforce strict performance of any provision of this Agreement or any right shall not be construed as a waiver of any such provision or right.

19. Class Action Waiver and Binding Arbitration

19.1. If you reside in the United States, this Clause 19 applies to you. If a dispute, claim, or controversy of any kind with respect to any Kaspersky Lab product, service, or any part of this agreement, arises between You and Kaspersky Lab or You and a third-party affiliate of Kaspersky Lab, and both parties couldn't resolve the dispute informally within a reasonable period of time, You and the other party agree to binding individual arbitration before the American Arbitration Association ("AAA") under the Federal Arbitration Act ("FAA"), and not to sue in court in front of a judge or jury. Any proceedings, including but not limited to class action lawsuits, class-wide arbitrations, private attorney-general actions, the combining of individual actions without the consent of all parties, or any other legal procedure where someone acts in a representative capacity, are not permitted. By accepting this agreement, You agree not to begin or participate in any of the above mentioned class and multi-party proceedings, and any action pursued by You and remedy, if any awarded to You, must be on an individual basis, as provided in this clause. In the event of a binding individual arbitration proceeding between parties, a neutral arbitrator will decide and the arbitrator’s decision will be final except for a limited right of appeal under the FAA. If any conflict exists between this agreement and the rules of the AAA, this agreement shall govern.

19.2. Any dispute, claim, or controversy concerning Kaspersky Lab's intellectual property rights, their enforcement, validity, etc., and any claim pertaining to any form of unauthorized use, including but not limited to theft and piracy, of any Kaspersky Lab product or service are not subject to this arbitration clause.

20. Rightholder Contact Information

Should you have any questions concerning this Agreement, or if you desire to contact the Rightholder for any reason, please contact our Customer Service Department at:

AO Kaspersky Lab, Bldg. 3, 39A, Leningradskoe Shosse
Moscow, 125212
Russian Federation
E-mail: info@kaspersky.com
Web site: www.kaspersky.com

Was this information helpful?
Yes No

Back to "Licensing and Activation"

Support for Home

Consumer Support Contacts
Contact support via My Kaspersky
Knowledge Base for Home
How-to Videos
Forum

Virus-fighting tools & services

Scan file or URL for viruses
Report a false alarm
Kaspersky Virus Removal Tool
Kaspersky Rescue Disk
Other virus-fighting tools

Support for Small Business

Small Business Support Contacts
Contact support via My Kaspersky
Knowledge Base for Small Business
Forum

Software Downloads

Buy online
Renew license
Get updates
Free trial download

Support terms and conditions
(updated April 12, 2017)

Support for Business

Business Support Contacts
Contact support via CompanyAccount
Knowledge Base for Business
Product Support Lifecycle
Premium Support Plans
Licensing by Subscription
Forum
Online Trainings
Subscribe to news

Site Feedback

Privacy Policy Contact Us About us

-
-
-
-
-
-

Have you found what you were looking for?

Please let us know how we can make this website more comfortable for you

Enter your feedback here (max. 500

Send feedback Send feedback

Thank you!

Thank you for submitting your feedback.
We will review your feedback shortly.

Exhibit 10

H. R. 2810

One Hundred Fifteenth Congress of the United States of America

AT THE FIRST SESSION

Begun and held at the City of Washington on Tuesday, the third day of January, two thousand and seventeen

An Act

To authorize appropriations for fiscal year 2018 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "National Defense Authorization Act for Fiscal Year 2018".

SEC. 2. ORGANIZATION OF ACT INTO DIVISIONS; TABLE OF CONTENTS.

(a) DIVISIONS.—This Act is organized into four divisions as follows:

(1) Division A—Department of Defense Authorizations.

(2) Division B—Military Construction Authorizations.

(3) Division C—Department of Energy National Security Authorizations and Other Authorizations.

(4) Division D—Funding Tables.

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

cyber activities that are carried out against infrastructure critical to the political integrity, economic security, and national security of the United States.

(4) Available or planned cyber capabilities that may be used to impose costs on any foreign power targeting the United States or United States persons with a cyber attack or malicious cyber activity.

(5) Development of multi-prong response options, such as—

(A) boosting the cyber resilience of critical United States strike systems (including cyber, nuclear, and non-nuclear systems) in order to ensure the United States can credibly threaten to impose unacceptable costs in response to even the most sophisticated large-scale cyber attack;

(B) developing offensive cyber capabilities and specific plans and strategies to put at risk targets most valued by adversaries of the United States and their key decision makers; and

(C) enhancing attribution capabilities and developing intelligence and offensive cyber capabilities to detect, disrupt, and potentially expose malicious cyber activities.

(c) LIMITATION ON AVAILABILITY OF FUNDS.—

(1) IN GENERAL.—Of the funds authorized to be appropriated by this Act or otherwise made available for fiscal year 2018 for procurement, research, development, test and evaluation, and operations and maintenance, for the covered activities of the Defense Information Systems Agency, not more than 60 percent may be obligated or expended until the date on which the President submits to the appropriate congressional committees the report under subsection (a)(2).

(2) COVERED ACTIVITIES DESCRIBED.—The covered activities referred to in paragraph (1) are the activities of the Defense Information Systems Agency in support of—

(A) the White House Communication Agency; and

(B) the White House Situation Support Staff.

(d) DEFINITIONS.—In this section:

(1) The term "foreign power" has the meaning given that term in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(2) The term "appropriate congressional committees" means—

(A) the congressional defense committees;

(B) the Committee on Foreign Affairs, the Committee on Homeland Security, and the Committee on the Judiciary of the House of Representatives; and

(C) the Committee on Foreign Relations, the Committee on Homeland Security and Governmental Affairs, and the Committee on the Judiciary of the Senate.

SEC. 1634. PROHIBITION ON USE OF PRODUCTS AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB.

(a) PROHIBITION.—No 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—

(1) Kaspersky Lab (or any successor entity);

(2) any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or

(3) any entity of which Kaspersky Lab has majority ownership.

(b) EFFECTIVE DATE.—The prohibition in subsection (a) shall take effect on October 1, 2018.

(c) REVIEW AND REPORT.—

(1) REVIEW.—The Secretary of Defense, in consultation with the Secretary of Energy, the Secretary of Homeland Security, the Attorney General, the Administrator of the General Services Administration, and the Director of National Intelligence, shall conduct a review of the procedures for removing suspect products or services from the information technology networks of the Federal Government.

(2) REPORT.—

(A) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, Secretary of Defense shall submit to the appropriate congressional committees a report on the review conducted under paragraph (1).

(B) ELEMENTS.—The report under subparagraph (A) shall include the following:

(i) A description of the 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, including—

(I) the discretionary authorities of agencies to prohibit, exclude, or prevent the use of such products or services;

(II) the authorities of a suspension and debarment official to prohibit, exclude, or prevent the use of such products or services;

(III) authorities relating to supply chain risk management;

(IV) authorities that provide for the continuous monitoring of information technology networks to identify suspect products or services; and

(V) the authorities provided under the Federal Information Security Management Act of 2002.

(ii) Assessment of any gaps in the authorities described in clause (i), including any gaps in the enforcement of decisions made under such authorities.

(iii) An explanation of the capabilities and methodologies used to periodically assess and monitor the information technology networks of the Federal Government for prohibited products or services.

(iv) An assessment of the ability of the Federal Government to periodically conduct training and exercises in the use of the authorities described in clause (i)—

(I) to identify recommendations for streamlining process; and

(II) to identify recommendations for education and training curricula, to be integrated into existing training or certification courses.

(v) A description of information sharing mechanisms that may be used to share information about suspect products or services, including mechanisms for the sharing of such information among the Federal Government, industry, the public, and international partners.

(vi) Identification of existing tools for business intelligence, application management, and commerce due-diligence that are either in use by elements of the Federal Government, or that are available commercially.

(vii) Recommendations for improving the authorities, processes, resourcing, and capabilities of the Federal Government for the purpose of improving the procedures for identifying and removing prohibited products or services from the information technology networks of the Federal Government.

(viii) Any other matters the Secretary determines to be appropriate.

(C) FORM.—The report under subparagraph (A) shall be submitted in unclassified form, but may include a classified annex.

(3) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this section, the term "appropriate congressional committees" means the following:

(A) The Committee on Armed Services, the Committee on Energy and Commerce, the Committee on Homeland Security, the Committee on the Judiciary, the Committee on Oversight and Government Reform, and the Permanent Select Committee on Intelligence of the House of Representatives.

(B) The Committee on Armed Services, the Committee on Energy and Natural Resources, the Committee on Homeland Security and Governmental Affairs, the Committee on the Judiciary, and the Select Committee on Intelligence of the Senate.

SEC. 1635. MODIFICATION OF AUTHORITIES RELATING TO ESTABLISHMENT OF UNIFIED COMBATANT COMMAND FOR CYBER OPERATIONS.

Section 167b of title 10, United States Code, is amended—

(1) by striking subsection (d); and

(2) by redesignating subsections (e) and (f) as subsections (d) and (e), respectively.

SEC. 1636. MODIFICATION OF DEFINITION OF ACQUISITION WORKFORCE TO INCLUDE PERSONNEL CONTRIBUTING TO CYBERSECURITY SYSTEMS.

Section 1705(h)(2)(A) of title 10, United States Code, is amended—

(1) by inserting "(i)" after "(A)";

(2) by striking "; and" and inserting "; or"; and

(3) by adding at the end the following new clause:

"(ii) contribute significantly to the acquisition or development of systems relating to cybersecurity; and".

Exhibit 11

Congress of the United States
House of Representatives

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6301
(202) 225–6371
www.science.house.gov

July 27, 2017

The Honorable Sonny Perdue
Secretary
U.S. Department of Agriculture
1400 Independence Avenue SW
Washington D.C. 20250

Dear Secretary Perdue,

As part of an ongoing review of the federal government's cybersecurity policies and standards, the Committee on Science, Space, and Technology is requesting information and documents from the Department regarding Kaspersky Lab. The Committee is charged with oversight of the National Institute of Standards and Technology (NIST), and continuously evaluates whether changes to the Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework) are necessary. The documents and information will assist the Committee in determining whether the Framework requires further refinement when implemented by federal departments and agencies.

Kaspersky Lab is among the world's largest cybersecurity companies. Headquartered in Moscow, Russia, it services approximately 400 million users worldwide, including a number of United States Government Agencies and entities.[1] Kaspersky Lab specializes in anti-virus software—products with potentially uninhibited access to the systems they protect.[2] Although Kaspersky Lab was once considered a reputable cybersecurity firm, several concerns have been raised regarding the company and Eugene Kaspersky—the founder and CEO of Kaspersky Lab—and his potential ties to the Russian government.

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. As early as 2015, reports began to surface

---

[1] *See* Jordan Robertson, *A Russian Cybersecurity Company's Ties to the Kremlin*, BLOOMBERG GOVERNMENT, Jul. 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSXAKB6JIJVL (last visited July 11, 2017).
[2] *See* Jordan Robertson & Michael Riley, *Kaspersky Lab Has Been Working With Russian Intelligence*, BLOOMBERG GOVERNMENT, July 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSX50G6KLVR5 (last visited July 11, 2017).

alleging that Mr. Kaspersky may have "close ties to Russian spies."[3] Shortly thereafter, *Reuters* reported that Kaspersky Lab engaged in a "sabotage" campaign undoubtedly targeting the U.S. cybersecurity market.[4] Specifically, the company "tried to damage rivals in the marketplace by tricking their antivirus software programs into classifying benign files as malicious."[5] More recently, Russia's alleged interference in the 2016 presidential election has heightened public concerns about the Kremlin's desire to meddle with American democratic processes. This, in turn, has ignited speculation over America's cybersecurity posture, and the potential ties that Kaspersky Lab has with the Kremlin. Namely, that the Russian government could use products manufactured by Kaspersky Lab as a medium for engaging in nefarious cyber campaigns against U.S. information systems—including those at several federal departments and agencies—that are purportedly protected by the company's products.[6] Adding to concern, the FBI sent agents to visit "at least a dozen employees of Kaspersky" in order to question them "about the company's operations as part of a counter-intelligence inquiry."[7]

Given the increasing prevalence of cybersecurity threats across the nation, the federal government's use of cybersecurity products manufactured by a firm with potential ties to the Russian government is concerning to Congress. In May, the Senate Intelligence Committee held an open hearing where several top U.S. intelligence officials stated with consensus that they would not be comfortable using Kaspersky Lab's products on their systems.[8] Additionally, on June 15, 2017, the House Science Committee Subcommittees on Oversight and Research and Technology held a joint hearing where cybersecurity experts testified on industry approaches and

---

[3] Carol Matlack, *The Company Securing Your Internet Has Close Ties to Russian Spies*, BLOOMBERG BUSINESSWEEK, Mar. 19, 2015, *available at* https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies (last visited June 19, 2017).

[4] Joseph Menn, *Exclusive: Russian Antivirus Firm Faked Malware to Harm Rivals*, REUTERS, Aug. 14, 2015, *available at* www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QJ1CR20150814 (last visited June 27, 2017); *see also* Joseph Menn, *Exclusive: Russia's Kaspersky Threatened to 'Rub Out' Rival, Email Shows*, REUTERS, Aug. 28, 2015, *available at* http://www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QX2GO20150828 (last visited June 27, 2017).

[5] *Id.*

[6] *See* Ali Watkins, *US Officials Are Warning About A Russian Cybersecurity Company's US Government Ties*, BUZZFEED NEWS, May 8, 2017, *available at* https://www.buzzfeed.com/alimwatkins/us-officials-are-warning-about-a-russian-cybersecurity?utm_term=.osyYrP2Mz6#.kexPnOw1Lk (last visited June 19, 2017); *see also* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).

[7] Ken Dilanian & Tom Winter, *Bill Would Bar Pentagon From Business With Russian Cyber Firm Kaspersky*, NBC NEWS, June 28, 2017, *available at* http://www.nbcnews.com/news/us-news/fbi-interviews-employees-russia-linked-cyber-security-firm-kaspersky-lab-n777571 (last visited June 29, 2017); *see also* Joe Uchill, *FBI Visits Kaspersky Lab Employees*, THE HILL, June 28, 2017, *available at* http://thehill.com/policy/cybersecurity/339887-fbi-visits-kaspersky-lab-employees (last visited June 29, 2017).

[8] S. Comm. on Intel., *Worldwide Threats Hearing*, 115th Cong. (May 11, 2017). (question and answer by Senator Marco Rubio).

best practices for safeguarding against future cyber threats.[9] Among the panel of expert witnesses was Salim Neino, CEO of Kryptos Logic—the cybersecurity firm whose employee helped thwart further propagation of the recent WannaCry ransomware attack.[10] In response to questions about the ability of a software manufacturer to embed a "backdoor" into anti-virus software—to facilitate a State's cyber-espionage activities—Mr. Neino alarmingly affirmed that he had "seen that a multitude of times" in the past, and that the barriers to engaging in such activities are "very low."[11] This revelation gives the Committee great concern, especially in light of the capabilities that anti-virus software possesses. Additionally, in response to a question regarding Kaspersky Lab, retired Army General Gregory Touhill, the first federal chief information security officer or CISO, told the Committee: "I buy American."[12]

Anti-virus software is extremely powerful and operates by scanning files at the system level, rather than on the network periphery.[13] As such, other security systems generally do not monitor the operations carried out by the anti-virus software.[14] From a practical perspective, this means that compromised anti-virus software could be used for malicious or nefarious purposes, and could do so without detection. If anti-virus technology or systems are compromised by a user's adversary, it could install malicious code disguised as a security update; it could forego specific updates to pave the way for use of certain vectors of attack; it could forego beneficial updates for a specified subset of users; and it could even extract data that a user's adversary considers valuable.[15] Furthermore, anti-virus is so powerful that it has nearly unimpeded access into all attachments, files, and information contained on a system.[16] In sum, compromised anti-virus has the potential to undermine the security and integrity of any system on which it is installed.

The security and integrity of federal information systems are only as strong as the products that guard them. Although Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, requires federal departments and agencies to implement the NIST Cybersecurity Framework and to provide reports related thereto,[17] the

---

[9] H. Comm. on Science, Space, & Tech. Subcomm. on Research & Tech. jointly with the Subcomm. on Oversight, *Hearing on Bolstering the Government's Cybersecurity: Lessons Learned from WannaCry*, Preliminary Hearing Transcript, 115th Cong. (June 15, 2017) at 61.
[10] *Id.*
[11] *Id.* at 62 (question and answer by Representative Clay Higgins).
[12] *Id.* at 63.
[13] *See* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] The White House, *Executive Order – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017), *available at* https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal (last visited June 29, 2017).

security of federal systems may nevertheless be undermined by compromised anti-virus products. Government contracting data indicating that several federal departments and agencies use or have used cybersecurity or anti-virus products manufactured by Kaspersky Lab is even more troubling.[18] If federal agencies and departments are being guarded by potentially compromised software, then it is virtually impossible for such agencies to effectively and efficiently implement the NIST Framework, and to fully comply with President Trump's executive order. The recent news that Kaspersky Lab's products have been removed from the General Service Administration's contracting Schedule 67 and 70 is encouraging, however federal agencies and contractors may be likely to continue use of Kaspersky Lab's products.[19]

Cybersecurity is a greater threat to our nation than ever before. If these widely reported allegations prove true, then the American public has ample grounds on which to rest their concerns about the security of data stored and transmitted on federal information systems—especially those allegedly protected by Kaspersky Lab's products. In light of this increasing threat, the Committee takes seriously its duty to ensure the NIST Cybersecurity Framework is properly equipped and adapted to safeguard our nation's information. To assist the Committee in understanding the effectiveness of the NIST Framework, and potential vulnerabilities that exist on federal information systems, please provide the following documents and information as soon as possible, but no later than August 11, 2017. Please provide the requested materials for the time frame from January 1, 2013, to present:

1. All documents and communications referring or relating to cybersecurity and/or anti-virus products manufactured by Kaspersky Lab.

2. All documents and communications referring or relating to any evaluation, risk assessment, and decision-making processes on the matter of whether to implement products manufactured by Kaspersky Lab.

3. All documents and communications referring or relating to the use or implementation of products manufactured by Kaspersky Lab.

---

[18] Government Contracting Dataset, *available at* https://www.usaspending.gov/Pages/AdvancedSearch.aspx?k=kaspersky (last visited June 29, 2017); *see* David Goldstein & Greg Gordon, *Exclusive: Kremlin Documents Suggest Link Between Cyber Giant and Russia Spy Agency*, MCCLATCHY, July 3, 2017, *available at* http://www.mcclatchydc.com/news/nation-world/national/article159342694.html (last visited July 12, 2017); *see also* Mike Levine & Pierre Thomas, *Officials Fear Russia Could Try To Target US Through Popular Software Firm Under FBI Scrutiny*, ABC NEWS, May 9, 2017, *available at* http://abcnews.go.com/US/officials-fear-russia-target-us-popular-software-firm/story?id=47295729 (last visited July 12, 2017).

[19] *See* Sarah Kuranda, *Kaspersky Lab Removed From GSA Schedule, Limiting Federal Sales for Its Security Software*, CRN, July 12, 2017, *available at* http://www.crn.com/news/security/300088591/kaspersky-removed-from-gsa-schedule-limiting-federal-sales-for-its-security-software.htm; *see also* Eric Geller, *Trump Administration Restricts Popular Russian Security Software*, POLITICO, July 11, 2017, *available at* http://www.politico.com/story/2017/07/11/trump-russian-security-software-240423.

4. A complete list of any computers, systems, data, media, and/or information utilizing or accessible to Kaspersky Lab products or services.

5. Identify any federal government contractors or subcontractors known to be utilizing Kaspersky Lab's products to fulfill requirements of contracts with the Department or Agency.

6. All documents and communications referring or relating to the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity.

7. All documents and communications referring or relating to the production of reports required by Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.

Pursuant to House Rule X, the Committee on Science, Space, and Technology has jurisdiction over National Institute of Standards and Technology which develops cybersecurity standards and guidelines for the federal government and recommendations for the private sector.

When producing documents to the Committee, please deliver production sets to the Majority Staff in Room 2321 of the Rayburn House Office Building and the Minority Staff in Room 394 of the Ford House Office Building. The Committee prefers, if possible, to receive all documents in electronic format.

If you have any questions about this request, please contact Drew Colliatie or Tom Connally at 202-225-6371. Thank you for your attention to this matter.

Sincerely,

Lamar Smith
Chairman

cc: The Honorable Eddie Bernice Johnson, Ranking Minority Member

Exhibit 12

10/25/2017 Hearing: Cybersecurity Posture
The Oversight Subcommittee of the
Committee on Science, Space, and Technology of the
U.S. House of Representatives

Introduction

Good morning Chairman LaHood, Ranking Member Beyer, and members of the Subcommittee. My name is David Shive, and I am the Chief Information Officer (CIO) of the U.S. General Services Administration (GSA). I welcome the opportunity to share my organization's experiences related to the cybersecurity posture of the Federal Government, specifically pertaining to the utilization of Kaspersky Lab products at Federal agencies, as well as the implementation of Executive Order 13800 and the NIST Cybersecurity Framework.

GSA Mission

The mission of GSA is to deliver the best value in real estate, acquisition, and technology services to Government and the American people. GSA's priorities are to deliver better value and savings, serve our partners, expand opportunities for small business, make Government more sustainable, and be a leader in innovation.

In support of that, and as it relates to the Subcommittee's objectives today, one of my organization's key goals in supporting GSA's mission is to deliver technology that provides a secure environment for doing business, while ensuring that both IT and business continue to run efficiently.

FISMA

The Federal Information Security Modernization Act of 2014 (FISMA) provides a comprehensive framework which helps Federal CIOs and Federal Chief Information Security Officers (CISOs) manage overall Information Technology (IT) security risks across Federal data and assets.

The FISMA framework supports the rigorous IT security program implemented at GSA by the CISO under the auspices of the CIO's authority. Our security program assures risks to GSA's IT systems are assessed and proper security controls implemented to mitigate those risks down to an acceptable level. It also provides a comprehensive policy, procedure, and governance structure, and ensures periodic evaluation and testing of the effectiveness of IT security controls, including management, operational, and technical controls. Further, all GSA employees take IT security awareness training; role-based training may also be required dependent on position and function.

Furthermore, GSA has a robust incident handling and response program that strongly aligns with the NIST Cybersecurity Framework. Due to the effectiveness of that program, GSA received a rating of Level 4 (Managed and Measurable) under "Response" on the latest FISMA report from the Office of Inspector General (OIG).

NIST Standards, FISMA and ATOs

In accordance with FISMA, GSA adheres to all of NIST's Federal Information Processing Standards (FIPS) and Special Publications (SP) in implementing GSA's IT security program. These include standards and guidance on encryption, security categorization of confidentiality, integrity, and availability (i.e., low, moderate, high), security control selection and implementation, risk management, authentication, identity management, system authorization, and contingency planning.

In addition, GSA completes a risk-based security assessment in accordance with NIST guidance and issues a signed Authority to Operate (ATO) by the authorizing official with concurrence by the CISO before any new system goes into production. The ATO is the official declaration that the IT systems can go live and be operated within an acceptable level of risk.

Cybersecurity Risk Management

Using the FISMA framework, along with NIST's Cybersecurity Framework, standards, and publications, GSA implements a risk-based strategy to manage IT security across the enterprise. Risk can never be completely eliminated, but the goal of GSA's IT security program is to allow GSA to provide services to its customers using information technology operated within an acceptable level of risk. This is accomplished by prioritizing the implementation of the security controls and focusing on those that have the biggest impact on securing the system and data. These include, but are not limited to: encryption, 2-factor authentication, ensuring secure configurations and patching of vulnerabilities, access controls, and auditing and monitoring.

Implementation of EO 13800 and the NIST Cybersecurity Framework

GSA is in the process of implementing Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017). GSA has adopted the framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by the National Institute of Standards and Technology, as required by the Executive Order. Specifically, GSA uses the Identify, Protect, Detect, Respond, and Recover areas of the NIST cybersecurity framework to better manage the overall risk to the agency.

In addition, GSA has provided a risk management report, as well as an action plan to implement the Framework, to the Secretary of Homeland Security and the Director of the Office of Management and Budget (OMB) per the Executive Order. The report identified GSA's highest risk areas along with risk mitigation and acceptance choices. GSA's program received

an overall evaluation of “Managing Risk” by the U.S. Department of Homeland Security (DHS) in their Cybersecurity Risk Management Assessment as part of the Executive Order.

GSA continues to explore leading edge technologies in order to stop the latest and most sophisticated attacks from our adversaries. These include next generation anti-virus solutions that use machine learning and artificial intelligence, as well as advanced detection of malware that is embedded in email attachments and links. This is done by doing in-depth analysis of the email before it reaches the end user. Both of these technologies will greatly protect the end user which is one of the primary vectors for exploiting Federal Government systems (otherwise known as phishing attacks).

GSA Role in Governmentwide IT Procurement

One of GSA’s core missions is to assist in procuring goods and services that can be made available to Federal agencies. GSA’s Federal Acquisition Service (FAS) offers a continuum of Governmentwide innovative solutions and services in a number of areas. Federal agencies spend approximately $23 billion annually to acquire IT products and services through FAS. This amount represents only 42 percent of the $54.8 billion in total contracted Federal IT spending across the entire Federal Government. As this figure indicates, Federal agencies are not required to use GSA contracts and, in fact, the majority of Federal IT spending does not occur through GSA.

Regardless of the acquisition vehicle used to acquire IT, as CIO it is my responsibility, as is the responsibility of any agency CIO, to ensure that we conduct a thorough examination of the IT solution and understand the risk of the product before we interface it with the existing agency IT infrastructure.

Significantly, a product’s placement on a GSA Multiple Award Schedule (Schedule) or other contract vehicle only certifies that the vendor meets the necessary contract and legal authority requirements for the product to be sold to the Federal Government; it does not make any value or technical judgment about the nature of the product. In the IT space, FISMA requires agency CIOs, such as myself, to make the determination for which products and solutions are appropriate for an agency’s environment.

With respect to Kaspersky Lab (KL) products, three resellers offered KL products through GSA Schedules contracts, but did not gain approval to do so via the required contract modification process. On July 11, 2017, GSA directed the three resellers to remove all KL manufactured products from their catalogs within 30 days. All three resellers complied. In addition, it is GSA’s understanding that on the same day, NASA and NIH, the other two Federal agencies with Governmentwide IT procurement contracts, removed Kaspersky manufactured products from their resellers’ catalogs. GSA does not offer any Kaspersky Lab manufactured products through its Schedules contracts.

Discovery and Removal of Kaspersky Products

GSA took a proactive stance and completed comprehensive scanning of all IT assets for the presence of KL products in June 2017. GSA confirmed that there was no installation of KL products in GSA's on-premise and cloud-based systems, and reported this to DHS in accordance with its Binding Operational Directive (BOD) 17-01 on October 4, 2017. GSA currently uses McAfee as its anti-virus provider.

In addition, GSA's Federal Risk and Authorization Management Program's (FedRAMP) Program Management Office is coordinating this activity for the Governmentwide Cloud Service Providers (CSPs) that are covered by FedRAMP ATOs.

Conclusion

Again, I thank you for allowing me the opportunity to contribute to this important topic. GSA appreciates this Committee's oversight of the Federal Government's cybersecurity posture on behalf of the American people.

At this time, I'm happy to take any questions that you might have.

Exhibit 13

POLITICO

Kaspersky has vehemently denied any connection to the Russian government, and strenuously objected to suggestions the Kremlin could use its products to spy on its American customers. | AP Photo

Trump administration restricts popular Russian security software

By **ERIC GELLER** | 07/11/2017 05:52 PM EDT | Updated 07/11/2017 05:39 PM EDT

The Trump administration has discouraged government agencies from using a leading Russian cybersecurity firm's software amid fears that the firm's products could serve as a Trojan horse for the Kremlin's hackers.

The General Services Administration said Tuesday that it had removed Kaspersky Lab from the approved list of vendors for two government-wide purchasing contracts that agencies use to acquire technology services.

"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," Donna Garland, a GSA spokeswoman, told POLITICO.

Agencies can still buy Kaspersky software outside the GSA contracts, but the process is more complex, and GSA's decision signaled a desire on the part of the administration to discourage the use of Kaspersky products.

Kaspersky has vehemently denied any connection to the Russian government, and strenuously objected to suggestions the Kremlin could use its products to spy on its American customers.

In a statement, the company said it "has no ties to any government" and "has never helped, nor will help, any government in the world with its cyberespionage efforts."

"Kaspersky Lab believes it is completely unacceptable that the company is being unjustly accused without any hard evidence to back up these false allegations," the company told POLITICO.

ABC News first reported Tuesday morning that the administration was considering blocking agencies from using Kaspersky software.

U.S. law enforcement and intelligence agencies have spent months investigating the possibility that Moscow could leverage its regulation of Russian companies to piggyback on

Kaspersky products and breach American networks.

The Department of Homeland Security issued a secret report on Kaspersky in February, and the FBI has interviewed Kaspersky's U.S. employees at their homes, according to ABC.

Trump calls son 'high-quality person' amid Russian lawyer scandal
By **MATTHEW NUSSBAUM**

The Senate Intelligence Committee has also asked the Justice Department and the Office of the Director of National Intelligence — which oversees all intelligence agencies — to investigate the matter, ABC said. Committee lawmakers were briefed on the matter in late May, and Senate lawmakers recently added a provision to the annual defense policy bill that would bar the Pentagon from installing Kaspersky software.

Government leaders are particularly sensitive to Russia's cyber menace in light of recent allegations that Moscow has deployed its hackers to infiltrate networks operating America's critical infrastructure, including the power grid and election-related systems. The Kremlin has also been accused of orchestrating breaches at numerous government agencies, such as the State Department, White House and Pentagon.

Bloomberg reported Tuesday that Kaspersky had a close relationship with Russia's Federal Security Service, or FSB, one of the two intelligence agencies that allegedly participated in the 2016 election cyberattacks. "It has developed security technology at the spy agency's behest," Bloomberg said, "and worked on joint projects the CEO knew would be embarrassing if made public."

GSA said it had removed Kaspersky from the list of approved vendors in the agency's Schedule 67 and Schedule 70 contracts, which cover digital imagery and IT services, respectively.

The ODNI declined to comment and the FBI did not immediately respond to a request for comment.

Exhibit 14

Proud to keep on protecting – no matter of false allegations in U.S. media

October 19, 2017

Eugene Kaspersky

11 posts

NEWS

SPECIAL PROJECTS

BANYA CIA

KASPERSKY LAB

MEDIA NSA

RUSSIAN HACKERS

SECURITY

Hi folks!

I doubt you'll have missed the unrelenting negative news coverage about KL of late. The most recent accusation is that alleged Russian hackers and the hidden hand of the Kremlin have somehow used our products to spy on American users and pilfer their secrets.

The media attacks have been intense, fierce and persistent – so much so that we've had to lay low for a while to catch our breath and work out what on earth this is all about. But now, since nearly a week has passed without any significant flak coming our way, I've been able to take the time to sit down and put fingertips to keyboard and assess the situation as objectively as I can. And I'd best do it quickly, since the respite may be short.

So, again... What exactly is going on here?

First up, let's keep in mind that concerns about KL, given its origins, are not new. We recognize that some people think 'Russian cybersecurity company' are three words that shouldn't be in the same sentence,

Clearly we're doing something right. And we want to continue doing it better – in the ongoing fight against cybercrime

especially these days. Still, the motivations behind recent reports, while intriguing, cannot be our concern. Instead, we need to focus on doing everything possible to be as transparent as possible for our most important stakeholders: our customers and partners.

Despite today's tense geopolitical situation, KL has continued do what it does best: focusing on protecting our customers from cyberthreats regardless of where those threats may come from. Our folks work hard every day to be the best at what they do in order to provide the best cybersecurity protection available. And independent tests and awards show that our efforts haven't been in vain. Just this month we were awarded the top 'Platinum Award' as part of the first ever Gartner Peer Insights Customer Choice Awards for Endpoint Protection Platforms. To receive any industry award is a good thing; to receive one based on what customers say about us is even better. Clearly we're doing something right. And we want to continue doing it right... no – better – in the ongoing fight against cybercrime.

If these recent allegations in U.S. media are true, where's the evidence?

But we know awards and accolades don't address these recent allegations. And we all know that government scrutiny of KL will continue. The past year has seen concerns about KL change from 'what if their technology could be a tool for cyber-espionage by nation states' to 'they were hacked and used as a vehicle to spy on spies'. And while it's hard for us to keep up with the constantly evolving narrative, ask yourself one thing: 'if these recent allegations are true, where's the evidence?' If there was any evidence that we've been knowingly involved in cyber-espionage, we'd be toast! No ifs or buts

– it'd be game over: governments would take immediate, severe action, including legal moves, and that would be that. But there's been nothing of the kind. And you have to wonder why.

Another issue is where's the due process? The steady stream of media leaks seem intentionally designed to damage our reputation without providing us with any real opportunity to address any concerns – because action is being taken before we can engage. Some will say that the government has provided us with an administrative remedy that we can pursue, and if so we will do so. But genuine due process provides you with the opportunity to defend yourself and see the evidence against you before action is taken; it doesn't ask you to respond once action is already underway.

We know that the allegations are very serious, and we're taking them very seriously. And since we aren't seeing the due process we'd expect, here, for now, let me at least put the record straight on a few technical matters that appear to have been misrepresented in the recent media reports – a few explanations of what it is our software *actually* does:

The functionality of our products depends entirely on the code of our applications and the records in our databases – no mysterious magic here (just like there's no mysterious magic with all other software companies' products). And all our products and databases are all openly accessible on public servers. All our old products and former updates – in backups. If in any of it there's any undeclared (espionage) functionality that violates the confidentiality of data of our users – do tell us the name of the product, the name of the module, and where the suspected code is, or the number of the update and the record identifier. That's the information we'd be ready to look at – with the utmost seriousness. If there's no information like that in any media report with accusations

aimed at us, such a report is based on known-to-be lies, or simply repeated lies and falsifications of someone else.

How our products work is determined exclusively by the logic of the algorithms in the program modules and contents of our databases. The last time we conducted a full audit of the source code of our products and database records was in spring-summer of 2015 since our own network had been compromised by the Duqu 2 espionage malware. And we found zero bugs, zero backdoors – not in our products, not in our databases, not in our updates. We're conducting a similar audit right now. And we're inviting external expert IT-security observers too. And I'm absolutely certain nothing untoward will be found.

Yes, our products do conduct deep scanning of a computer and its files (as does all software in the 'utility' category). We do test files for the presence of malicious code. We do specially track and evaluate suspicious behavior of unknown objects in a system. And yes, we do – in full accordance with declared functionality and industry standards – send data on such objects to the cloud for further analysis (if the user has decided to go for this option). And this is how any antivirus worth its salt works. Any why? It's all for one purpose: a finely-tuned, fully-optimized ability to do nothing but catch malware, neutralize it, and so protect our users. And we happen to be the best in the world at it. Our mission is to protect our users and their data. Surveillance, snooping, spying, eavesdropping... all that is done by espionage agencies (which we occasionally catch out and tell the world about), not us.

In the cyberworld, evidence usually means the names of the respective modules, location of the code, and its disassembler (or its part).

The main priority of our company is the protection of our

Indeed, it's details like these that make up the main findings in our expert reports on the world's most complex cyber-incidents (more on those – here).

users from all types of cyberthreats, no matter their origin.

Again, we remain absolutely committed to the protection of our users, and we work hard every day to do it better than anyone else. We've asked those with any relevant information to share it with us so we can do everything possible to fulfill our mission. Buy one of our boxed products in the nearest supermarket or an online version – analyze it, decompile it, and let us hear your findings! But we know we can't wait for folks to come to us. Therefore, we'll do everything we can to respond to the stated concerns by being fully transparent about our efforts and our findings. Our customers deserve nothing less.

In closing, I once again declare:

The main priority of our company is the protection of our users from all types of cyberthreats, no matter their origin. We do this better than anyone else. And that's nothing to be ashamed of – only proud of.

Sincerely yours,
E.K.

Explainer: Smart contracts, Ethereum, ICO

Transatlantic Cable podcast, episode 7

Read Next