

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.

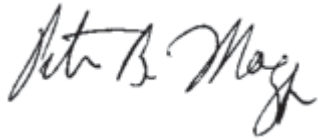
54. The Request goes on to state:

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,

A handwritten signature in cursive script, reading "Peter B. Maggs".

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, Subcommittee 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 Zhiltsov) *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 of 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: Transnational 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 F.J.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, Rechtsvereinheitlichung; 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 internationale de droit comparé- International Academy of Comparative Law, *Rapports Généraux XIIIe Congrès 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 XIIIth 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: Etablissements 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: Etablissements 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.

"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. deBessonnet) "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 Transition: 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 Nineteenth 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 I): 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 Mestmeyer (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, *Eigentumsordnung und Technologiepolitik. Eine system-vergleichende 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 Geburtenzahl*. *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, *Juristische 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. Kuchеров, *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.

TLP:AMBER



REPORT:

**Supplemental Information
Security Risk Assessment**

NUMBER

DATE

Kaspersky-Branded Products and Berkeley Research Group Independent Assessment



NCCIC

TLP:AMBER

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 (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 (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.

WARNING: This document is UNCLASSIFIED//For Official Use Only (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with the DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need to know" without prior approval of an authorized DHS office.

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:

- Sec. 1. Short title.
Sec. 2. Organization of Act into divisions; table of contents.
Sec. 3. Congressional defense committees.
Sec. 4. Budgetary effects of this Act.

DIVISION A—DEPARTMENT OF DEFENSE AUTHORIZATIONS

TITLE I—PROCUREMENT

Subtitle A—Authorization Of Appropriations

Sec. 101. Authorization of appropriations.

Subtitle B—Army Programs

- Sec. 111. Authority to expedite procurement of 7.62mm rifles.
Sec. 112. Limitation on availability of funds for Increment 2 of the Warfighter Information Network-Tactical program.
Sec. 113. Limitation on availability of funds for upgrade of M113 vehicles.

Subtitle C—Navy Programs

- Sec. 121. Aircraft carriers.
Sec. 122. Icebreaker vessel.
Sec. 123. Multiyear procurement authority for Arleigh Burke class destroyers.
Sec. 124. Multiyear procurement authority for Virginia class submarine program.
Sec. 125. Design and construction of the lead ship of the amphibious ship replacement designated LX(R) or amphibious transport dock designated LPD-30.
Sec. 126. Multiyear procurement authority for V-22 Osprey aircraft.
Sec. 127. Extension of limitation on use of sole-source shipbuilding contracts for certain vessels.

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—

H. R. 2810—458

- (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”.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

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




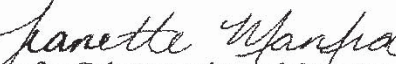
**Homeland
Security**

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 systems² 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).

UNCLASSIFIED//FOR OFFICIAL USE ONLY

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>.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

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.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

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).

UNCLASSIFIED//FOR OFFICIAL USE ONLY

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>).

UNCLASSIFIED//FOR OFFICIAL USE ONLY

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>).

UNCLASSIFIED//FOR OFFICIAL USE ONLY

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](https://www.dni.gov/files/documents/Unclassified%202015%20ATA%20SFR%20-%20SASC%20FINAL.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](https://www.dni.gov/files/documents/ICA%202017%2001.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/usc-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.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

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

UNCLASSIFIED//FOR OFFICIAL USE ONLY

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 Apple 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).

UNCLASSIFIED//FOR OFFICIAL USE ONLY

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/kaspersky-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](http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2012)015-e)) (quoting CDL-AD(2007)016).

UNCLASSIFIED//FOR OFFICIAL USE ONLY

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).

UNCLASSIFIED//FOR OFFICIAL USE ONLY

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

UNCLASSIFIED//FOR OFFICIAL USE ONLY

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

UNCLASSIFIED//FOR OFFICIAL USE ONLY

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 country'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>).

UNCLASSIFIED//FOR OFFICIAL USE ONLY

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).

UNCLASSIFIED//FOR OFFICIAL USE ONLY

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.

