LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6301
(202) 225-6371
www.science.house.gov

July 27, 2017

The Honorable Sonny Perdue
Secretary
U.S. Department of Agriculture
1400 Independence Avenue SW
Washington D.C. 20250

Dear Secretary Perdue,

As part of an ongoing review of the federal government's cybersecurity policies and standards, the Committee on Science, Space, and Technology is requesting information and documents from the Department regarding Kaspersky Lab. The Committee is charged with oversight of the National Institute of Standards and Technology (NIST), and continuously evaluates whether changes to the Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework) are necessary. The documents and information will assist the Committee in determining whether the Framework requires further refinement when implemented by federal departments and agencies.

Kaspersky Lab is among the world's largest cybersecurity companies. Headquartered in Moscow, Russia, it services approximately 400 million users worldwide, including a number of United States Government Agencies and entities.[1] Kaspersky Lab specializes in anti-virus software—products with potentially uninhibited access to the systems they protect.[2] Although Kaspersky Lab was once considered a reputable cybersecurity firm, several concerns have been raised regarding the company and Eugene Kaspersky—the founder and CEO of Kaspersky Lab—and his potential ties to the Russian government.

The Committee is concerned that Kaspersky Lab is susceptible to manipulation by the Russian government, and that its products could be used as a tool for espionage, sabotage, or other nefarious activities against the United States. As early as 2015, reports began to surface

---

[1] *See* Jordan Robertson, *A Russian Cybersecurity Company's Ties to the Kremlin*, BLOOMBERG GOVERNMENT, Jul. 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSXAKB6JIJVL (last visited July 11, 2017).
[2] *See* Jordan Robertson & Michael Riley, *Kaspersky Lab Has Been Working With Russian Intelligence*, BLOOMBERG GOVERNMENT, July 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSX50G6KLVR5 (last visited July 11, 2017).

alleging that Mr. Kaspersky may have "close ties to Russian spies."[3] Shortly thereafter, *Reuters* reported that Kaspersky Lab engaged in a "sabotage" campaign undoubtedly targeting the U.S. cybersecurity market.[4] Specifically, the company "tried to damage rivals in the marketplace by tricking their antivirus software programs into classifying benign files as malicious."[5] More recently, Russia's alleged interference in the 2016 presidential election has heightened public concerns about the Kremlin's desire to meddle with American democratic processes. This, in turn, has ignited speculation over America's cybersecurity posture, and the potential ties that Kaspersky Lab has with the Kremlin. Namely, that the Russian government could use products manufactured by Kaspersky Lab as a medium for engaging in nefarious cyber campaigns against U.S. information systems—including those at several federal departments and agencies—that are purportedly protected by the company's products.[6] Adding to concern, the FBI sent agents to visit "at least a dozen employees of Kaspersky" in order to question them "about the company's operations as part of a counter-intelligence inquiry."[7]

Given the increasing prevalence of cybersecurity threats across the nation, the federal government's use of cybersecurity products manufactured by a firm with potential ties to the Russian government is concerning to Congress. In May, the Senate Intelligence Committee held an open hearing where several top U.S. intelligence officials stated with consensus that they would not be comfortable using Kaspersky Lab's products on their systems.[8] Additionally, on June 15, 2017, the House Science Committee Subcommittees on Oversight and Research and Technology held a joint hearing where cybersecurity experts testified on industry approaches and

---

[3] Carol Matlack, *The Company Securing Your Internet Has Close Ties to Russian Spies*, BLOOMBERG BUSINESSWEEK, Mar. 19, 2015, *available at* https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies (last visited June 19, 2017).

[4] Joseph Menn, *Exclusive: Russian Antivirus Firm Faked Malware to Harm Rivals*, REUTERS, Aug. 14, 2015, *available at* www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QJ1CR20150814 (last visited June 27, 2017); *see also* Joseph Menn, *Exclusive: Russia's Kaspersky Threatened to 'Rub Out' Rival, Email Shows*, REUTERS, Aug. 28, 2015, *available at* http://www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QX2GO20150828 (last visited June 27, 2017).

[5] *Id.*

[6] *See* Ali Watkins, *US Officials Are Warning About A Russian Cybersecurity Company's US Government Ties*, BUZZFEED NEWS, May 8, 2017, *available at* https://www.buzzfeed.com/alimwatkins/us-officials-are-warning-about-a-russian-cybersecurity?utm_term=.osyYrP2Mz6#.kexPnOw1Lk (last visited June 19, 2017); *see also* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).

[7] Ken Dilanian & Tom Winter, *Bill Would Bar Pentagon From Business With Russian Cyber Firm Kaspersky*, NBC NEWS, June 28, 2017, *available at* http://www.nbcnews.com/news/us-news/fbi-interviews-employees-russia-linked-cyber-security-firm-kaspersky-lab-n777571 (last visited June 29, 2017); *see also* Joe Uchill, *FBI Visits Kaspersky Lab Employees*, THE HILL, June 28, 2017, *available at* http://thehill.com/policy/cybersecurity/339887-fbi-visits-kaspersky-lab-employees (last visited June 29, 2017).

[8] S. Comm. on Intel., *Worldwide Threats Hearing*, 115th Cong. (May 11, 2017). (question and answer by Senator Marco Rubio).

best practices for safeguarding against future cyber threats.[9] Among the panel of expert witnesses was Salim Neino, CEO of Kryptos Logic—the cybersecurity firm whose employee helped thwart further propagation of the recent WannaCry ransomware attack.[10] In response to questions about the ability of a software manufacturer to embed a "backdoor" into anti-virus software—to facilitate a State's cyber-espionage activities—Mr. Neino alarmingly affirmed that he had "seen that a multitude of times" in the past, and that the barriers to engaging in such activities are "very low."[11] This revelation gives the Committee great concern, especially in light of the capabilities that anti-virus software possesses. Additionally, in response to a question regarding Kaspersky Lab, retired Army General Gregory Touhill, the first federal chief information security officer or CISO, told the Committee: "I buy American."[12]

Anti-virus software is extremely powerful and operates by scanning files at the system level, rather than on the network periphery.[13] As such, other security systems generally do not monitor the operations carried out by the anti-virus software.[14] From a practical perspective, this means that compromised anti-virus software could be used for malicious or nefarious purposes, and could do so without detection. If anti-virus technology or systems are compromised by a user's adversary, it could install malicious code disguised as a security update; it could forego specific updates to pave the way for use of certain vectors of attack; it could forego beneficial updates for a specified subset of users; and it could even extract data that a user's adversary considers valuable.[15] Furthermore, anti-virus is so powerful that it has nearly unimpeded access into all attachments, files, and information contained on a system.[16] In sum, compromised anti-virus has the potential to undermine the security and integrity of any system on which it is installed.

The security and integrity of federal information systems are only as strong as the products that guard them. Although Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, requires federal departments and agencies to implement the NIST Cybersecurity Framework and to provide reports related thereto,[17] the

---

[9] H. Comm. on Science, Space, & Tech. Subcomm. on Research & Tech. jointly with the Subcomm. on Oversight, *Hearing on Bolstering the Government's Cybersecurity: Lessons Learned from WannaCry*, Preliminary Hearing Transcript, 115th Cong. (June 15, 2017) at 61.
[10] *Id.*
[11] *Id.* at 62 (question and answer by Representative Clay Higgins).
[12] *Id.* at 63.
[13] *See* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] The White House, *Executive Order – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017), *available at* https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal (last visited June 29, 2017).

security of federal systems may nevertheless be undermined by compromised anti-virus products. Government contracting data indicating that several federal departments and agencies use or have used cybersecurity or anti-virus products manufactured by Kaspersky Lab is even more troubling.[18] If federal agencies and departments are being guarded by potentially compromised software, then it is virtually impossible for such agencies to effectively and efficiently implement the NIST Framework, and to fully comply with President Trump's executive order. The recent news that Kaspersky Lab's products have been removed from the General Service Administration's contracting Schedule 67 and 70 is encouraging, however federal agencies and contractors may be likely to continue use of Kaspersky Lab's products.[19]

Cybersecurity is a greater threat to our nation than ever before. If these widely reported allegations prove true, then the American public has ample grounds on which to rest their concerns about the security of data stored and transmitted on federal information systems—especially those allegedly protected by Kaspersky Lab's products. In light of this increasing threat, the Committee takes seriously its duty to ensure the NIST Cybersecurity Framework is properly equipped and adapted to safeguard our nation's information. To assist the Committee in understanding the effectiveness of the NIST Framework, and potential vulnerabilities that exist on federal information systems, please provide the following documents and information as soon as possible, but no later than August 11, 2017. Please provide the requested materials for the time frame from January 1, 2013, to present:

1. All documents and communications referring or relating to cybersecurity and/or anti-virus products manufactured by Kaspersky Lab.

2. All documents and communications referring or relating to any evaluation, risk assessment, and decision-making processes on the matter of whether to implement products manufactured by Kaspersky Lab.

3. All documents and communications referring or relating to the use or implementation of products manufactured by Kaspersky Lab.

---

[18] Government Contracting Dataset, *available at* https://www.usaspending.gov/Pages/AdvancedSearch.aspx?k=kaspersky (last visited June 29, 2017); *see* David Goldstein & Greg Gordon, *Exclusive: Kremlin Documents Suggest Link Between Cyber Giant and Russia Spy Agency*, MCCLATCHY, July 3, 2017, *available at* http://www.mcclatchydc.com/news/nation-world/national/article159342694.html (last visited July 12, 2017); *see also* Mike Levine & Pierre Thomas, *Officials Fear Russia Could Try To Target US Through Popular Software Firm Under FBI Scrutiny*, ABC NEWS, May 9, 2017, *available at* http://abcnews.go.com/US/officials-fear-russia-target-us-popular-software-firm/story?id=47295729 (last visited July 12, 2017).

[19] *See* Sarah Kuranda, *Kaspersky Lab Removed From GSA Schedule, Limiting Federal Sales for Its Security Software*, CRN, July 12, 2017, *available at* http://www.crn.com/news/security/300088591/kaspersky-removed-from-gsa-schedule-limiting-federal-sales-for-its-security-software.htm; *see also* Eric Geller, *Trump Administration Restricts Popular Russian Security Software*, POLITICO, July 11, 2017, *available at* http://www.politico.com/story/2017/07/11/trump-russian-security-software-240423.

4. A complete list of any computers, systems, data, media, and/or information utilizing or accessible to Kaspersky Lab products or services.

5. Identify any federal government contractors or subcontractors known to be utilizing Kaspersky Lab's products to fulfill requirements of contracts with the Department or Agency.

6. All documents and communications referring or relating to the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity.

7. All documents and communications referring or relating to the production of reports required by Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.

Pursuant to House Rule X, the Committee on Science, Space, and Technology has jurisdiction over National Institute of Standards and Technology which develops cybersecurity standards and guidelines for the federal government and recommendations for the private sector.

When producing documents to the Committee, please deliver production sets to the Majority Staff in Room 2321 of the Rayburn House Office Building and the Minority Staff in Room 394 of the Ford House Office Building. The Committee prefers, if possible, to receive all documents in electronic format.

If you have any questions about this request, please contact Drew Colliatie or Tom Connally at 202-225-6371. Thank you for your attention to this matter.

Sincerely,

Lamar Smith
Chairman

cc: The Honorable Eddie Bernice Johnson, Ranking Minority Member

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6301
(202) 225–6371
www.science.house.gov

July 27, 2017

The Honorable Heather Wilson
Secretary
U.S. Department of Air Force
1690 Air Force Pentagon
Washington D.C. 20330 - 1670

Dear Secretary Wilson,

As part of an ongoing review of the federal government's cybersecurity policies and standards, the Committee on Science, Space, and Technology is requesting information and documents from the Department regarding Kaspersky Lab. The Committee is charged with oversight of the National Institute of Standards and Technology (NIST), and continuously evaluates whether changes to the Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework) are necessary. The documents and information will assist the Committee in determining whether the Framework requires further refinement when implemented by federal departments and agencies.

Kaspersky Lab is among the world's largest cybersecurity companies. Headquartered in Moscow, Russia, it services approximately 400 million users worldwide, including a number of United States Government Agencies and entities.[1] Kaspersky Lab specializes in anti-virus software—products with potentially uninhibited access to the systems they protect.[2] Although Kaspersky Lab was once considered a reputable cybersecurity firm, several concerns have been raised regarding the company and Eugene Kaspersky—the founder and CEO of Kaspersky Lab—and his potential ties to the Russian government.

The Committee is concerned that Kaspersky Lab is susceptible to manipulation by the Russian government, and that its products could be used as a tool for espionage, sabotage, or other nefarious activities against the United States. As early as 2015, reports began to surface

---

[1] *See* Jordan Robertson, *A Russian Cybersecurity Company's Ties to the Kremlin*, BLOOMBERG GOVERNMENT, Jul. 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSXAKB6JIJVL (last visited July 11, 2017).
[2] *See* Jordan Robertson & Michael Riley, *Kaspersky Lab Has Been Working With Russian Intelligence*, BLOOMBERG GOVERNMENT, July 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSX50G6KLVR5 (last visited July 11, 2017).

alleging that Mr. Kaspersky may have "close ties to Russian spies."[3] Shortly thereafter, *Reuters* reported that Kaspersky Lab engaged in a "sabotage" campaign undoubtedly targeting the U.S. cybersecurity market.[4] Specifically, the company "tried to damage rivals in the marketplace by tricking their antivirus software programs into classifying benign files as malicious."[5] More recently, Russia's alleged interference in the 2016 presidential election has heightened public concerns about the Kremlin's desire to meddle with American democratic processes. This, in turn, has ignited speculation over America's cybersecurity posture, and the potential ties that Kaspersky Lab has with the Kremlin. Namely, that the Russian government could use products manufactured by Kaspersky Lab as a medium for engaging in nefarious cyber campaigns against U.S. information systems—including those at several federal departments and agencies—that are purportedly protected by the company's products.[6] Adding to concern, the FBI sent agents to visit "at least a dozen employees of Kaspersky" in order to question them "about the company's operations as part of a counter-intelligence inquiry."[7]

Given the increasing prevalence of cybersecurity threats across the nation, the federal government's use of cybersecurity products manufactured by a firm with potential ties to the Russian government is concerning to Congress. In May, the Senate Intelligence Committee held an open hearing where several top U.S. intelligence officials stated with consensus that they would not be comfortable using Kaspersky Lab's products on their systems.[8] Additionally, on June 15, 2017, the House Science Committee Subcommittees on Oversight and Research and Technology held a joint hearing where cybersecurity experts testified on industry approaches and

---

[3] Carol Matlack, *The Company Securing Your Internet Has Close Ties to Russian Spies*, BLOOMBERG BUSINESSWEEK, Mar. 19, 2015, *available at* https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies (last visited June 19, 2017).

[4] Joseph Menn, *Exclusive: Russian Antivirus Firm Faked Malware to Harm Rivals*, REUTERS, Aug. 14, 2015, *available at* www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QJ1CR20150814 (last visited June 27, 2017); *see also* Joseph Menn, *Exclusive: Russia's Kaspersky Threatened to 'Rub Out' Rival, Email Shows*, REUTERS, Aug. 28, 2015, *available at* http://www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QX2GO20150828 (last visited June 27, 2017).

[5] *Id.*

[6] *See* Ali Watkins, *US Officials Are Warning About A Russian Cybersecurity Company's US Government Ties*, BUZZFEED NEWS, May 8, 2017, *available at* https://www.buzzfeed.com/alimwatkins/us-officials-are-warning-about-a-russian-cybersecurity?utm_term=.osyYrP2Mz6#.kexPnOw1Lk (last visited June 19, 2017); *see also* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).

[7] Ken Dilanian & Tom Winter, *Bill Would Bar Pentagon From Business With Russian Cyber Firm Kaspersky*, NBC NEWS, June 28, 2017, *available at* http://www.nbcnews.com/news/us-news/fbi-interviews-employees-russia-linked-cyber-security-firm-kaspersky-lab-n777571 (last visited June 29, 2017); *see also* Joe Uchill, *FBI Visits Kaspersky Lab Employees*, THE HILL, June 28, 2017, *available at* http://thehill.com/policy/cybersecurity/339887-fbi-visits-kaspersky-lab-employees (last visited June 29, 2017).

[8] S. Comm. on Intel., *Worldwide Threats Hearing*, 115th Cong. (May 11, 2017). (question and answer by Senator Marco Rubio).

best practices for safeguarding against future cyber threats.[9] Among the panel of expert witnesses was Salim Neino, CEO of Kryptos Logic—the cybersecurity firm whose employee helped thwart further propagation of the recent WannaCry ransomware attack.[10] In response to questions about the ability of a software manufacturer to embed a "backdoor" into anti-virus software—to facilitate a State's cyber-espionage activities—Mr. Neino alarmingly affirmed that he had "seen that a multitude of times" in the past, and that the barriers to engaging in such activities are "very low."[11] This revelation gives the Committee great concern, especially in light of the capabilities that anti-virus software possesses. Additionally, in response to a question regarding Kaspersky Lab, retired Army General Gregory Touhill, the first federal chief information security officer or CISO, told the Committee: "I buy American."[12]

Anti-virus software is extremely powerful and operates by scanning files at the system level, rather than on the network periphery.[13] As such, other security systems generally do not monitor the operations carried out by the anti-virus software.[14] From a practical perspective, this means that compromised anti-virus software could be used for malicious or nefarious purposes, and could do so without detection. If anti-virus technology or systems are compromised by a user's adversary, it could install malicious code disguised as a security update; it could forego specific updates to pave the way for use of certain vectors of attack; it could forego beneficial updates for a specified subset of users; and it could even extract data that a user's adversary considers valuable.[15] Furthermore, anti-virus is so powerful that it has nearly unimpeded access into all attachments, files, and information contained on a system.[16] In sum, compromised anti-virus has the potential to undermine the security and integrity of any system on which it is installed.

The security and integrity of federal information systems are only as strong as the products that guard them. Although Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, requires federal departments and agencies to implement the NIST Cybersecurity Framework and to provide reports related thereto,[17] the

---

[9] H. Comm. on Science, Space, & Tech. Subcomm. on Research & Tech. jointly with the Subcomm. on Oversight, *Hearing on Bolstering the Government's Cybersecurity: Lessons Learned from WannaCry*, Preliminary Hearing Transcript, 115th Cong. (June 15, 2017) at 61.
[10] *Id.*
[11] *Id.* at 62 (question and answer by Representative Clay Higgins).
[12] *Id.* at 63.
[13] *See* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] The White House, *Executive Order – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017), *available at* https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal (last visited June 29, 2017).

security of federal systems may nevertheless be undermined by compromised anti-virus products. Government contracting data indicating that several federal departments and agencies use or have used cybersecurity or anti-virus products manufactured by Kaspersky Lab is even more troubling.[18] If federal agencies and departments are being guarded by potentially compromised software, then it is virtually impossible for such agencies to effectively and efficiently implement the NIST Framework, and to fully comply with President Trump's executive order. The recent news that Kaspersky Lab's products have been removed from the General Service Administration's contracting Schedule 67 and 70 is encouraging, however federal agencies and contractors may be likely to continue use of Kaspersky Lab's products.[19]

Cybersecurity is a greater threat to our nation than ever before. If these widely reported allegations prove true, then the American public has ample grounds on which to rest their concerns about the security of data stored and transmitted on federal information systems—especially those allegedly protected by Kaspersky Lab's products. In light of this increasing threat, the Committee takes seriously its duty to ensure the NIST Cybersecurity Framework is properly equipped and adapted to safeguard our nation's information. To assist the Committee in understanding the effectiveness of the NIST Framework, and potential vulnerabilities that exist on federal information systems, please provide the following documents and information as soon as possible, but no later than August 11, 2017. Please provide the requested materials for the time frame from January 1, 2013, to present:

1. All documents and communications referring or relating to cybersecurity and/or anti-virus products manufactured by Kaspersky Lab.

2. All documents and communications referring or relating to any evaluation, risk assessment, and decision-making processes on the matter of whether to implement products manufactured by Kaspersky Lab.

3. All documents and communications referring or relating to the use or implementation of products manufactured by Kaspersky Lab.

---

[18] Government Contracting Dataset, *available at* https://www.usaspending.gov/Pages/AdvancedSearch.aspx?k=kaspersky (last visited June 29, 2017); *see* David Goldstein & Greg Gordon, *Exclusive: Kremlin Documents Suggest Link Between Cyber Giant and Russia Spy Agency*, MCCLATCHY, July 3, 2017, *available at* http://www.mcclatchydc.com/news/nation-world/national/article159342694.html (last visited July 12, 2017); *see also* Mike Levine & Pierre Thomas, *Officials Fear Russia Could Try To Target US Through Popular Software Firm Under FBI Scrutiny*, ABC NEWS, May 9, 2017, *available at* http://abcnews.go.com/US/officials-fear-russia-target-us-popular-software-firm/story?id=47295729 (last visited July 12, 2017).

[19] *See* Sarah Kuranda, *Kaspersky Lab Removed From GSA Schedule, Limiting Federal Sales for Its Security Software*, CRN, July 12, 2017, *available at* http://www.crn.com/news/security/300088591/kaspersky-removed-from-gsa-schedule-limiting-federal-sales-for-its-security-software.htm; *see also* Eric Geller, *Trump Administration Restricts Popular Russian Security Software*, POLITICO, July 11, 2017, *available at* http://www.politico.com/story/2017/07/11/trump-russian-security-software-240423.

4. A complete list of any computers, systems, data, media, and/or information utilizing or accessible to Kaspersky Lab products or services.

5. Identify any federal government contractors or subcontractors known to be utilizing Kaspersky Lab's products to fulfill requirements of contracts with the Department or Agency.

6. All documents and communications referring or relating to the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity.

7. All documents and communications referring or relating to the production of reports required by Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.

Pursuant to House Rule X, the Committee on Science, Space, and Technology has jurisdiction over National Institute of Standards and Technology which develops cybersecurity standards and guidelines for the federal government and recommendations for the private sector.

When producing documents to the Committee, please deliver production sets to the Majority Staff in Room 2321 of the Rayburn House Office Building and the Minority Staff in Room 394 of the Ford House Office Building. The Committee prefers, if possible, to receive all documents in electronic format.

If you have any questions about this request, please contact Drew Colliatie or Tom Connally at 202-225-6371. Thank you for your attention to this matter.

Sincerely,

Lamar Smith
Chairman

cc: The Honorable Eddie Bernice Johnson, Ranking Minority Member

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6301
(202) 225–6371
www.science.house.gov

July 27, 2017

The Honorable Robert M. Speer
Acting Secretary
U.S. Department of Army
300 Army Pentagon
Washington D.C. 20310 - 0300

Dear Acting Secretary Speer,

As part of an ongoing review of the federal government's cybersecurity policies and standards, the Committee on Science, Space, and Technology is requesting information and documents from the Department regarding Kaspersky Lab. The Committee is charged with oversight of the National Institute of Standards and Technology (NIST), and continuously evaluates whether changes to the Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework) are necessary. The documents and information will assist the Committee in determining whether the Framework requires further refinement when implemented by federal departments and agencies.

Kaspersky Lab is among the world's largest cybersecurity companies. Headquartered in Moscow, Russia, it services approximately 400 million users worldwide, including a number of United States Government Agencies and entities.[1] Kaspersky Lab specializes in anti-virus software—products with potentially uninhibited access to the systems they protect.[2] Although Kaspersky Lab was once considered a reputable cybersecurity firm, several concerns have been raised regarding the company and Eugene Kaspersky—the founder and CEO of Kaspersky Lab—and his potential ties to the Russian government.

The Committee is concerned that Kaspersky Lab is susceptible to manipulation by the Russian government, and that its products could be used as a tool for espionage, sabotage, or other nefarious activities against the United States. As early as 2015, reports began to surface

---

[1] *See* Jordan Robertson, *A Russian Cybersecurity Company's Ties to the Kremlin*, BLOOMBERG GOVERNMENT, Jul. 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSXAKB6JIJVL (last visited July 11, 2017).
[2] *See* Jordan Robertson & Michael Riley, *Kaspersky Lab Has Been Working With Russian Intelligence*, BLOOMBERG GOVERNMENT, July 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSX50G6KLVR5 (last visited July 11, 2017).

alleging that Mr. Kaspersky may have "close ties to Russian spies."[3] Shortly thereafter, *Reuters* reported that Kaspersky Lab engaged in a "sabotage" campaign undoubtedly targeting the U.S. cybersecurity market.[4] Specifically, the company "tried to damage rivals in the marketplace by tricking their antivirus software programs into classifying benign files as malicious."[5] More recently, Russia's alleged interference in the 2016 presidential election has heightened public concerns about the Kremlin's desire to meddle with American democratic processes. This, in turn, has ignited speculation over America's cybersecurity posture, and the potential ties that Kaspersky Lab has with the Kremlin. Namely, that the Russian government could use products manufactured by Kaspersky Lab as a medium for engaging in nefarious cyber campaigns against U.S. information systems—including those at several federal departments and agencies—that are purportedly protected by the company's products.[6] Adding to concern, the FBI sent agents to visit "at least a dozen employees of Kaspersky" in order to question them "about the company's operations as part of a counter-intelligence inquiry."[7]

Given the increasing prevalence of cybersecurity threats across the nation, the federal government's use of cybersecurity products manufactured by a firm with potential ties to the Russian government is concerning to Congress. In May, the Senate Intelligence Committee held an open hearing where several top U.S. intelligence officials stated with consensus that they would not be comfortable using Kaspersky Lab's products on their systems.[8] Additionally, on June 15, 2017, the House Science Committee Subcommittees on Oversight and Research and Technology held a joint hearing where cybersecurity experts testified on industry approaches and

---

[3] Carol Matlack, *The Company Securing Your Internet Has Close Ties to Russian Spies*, BLOOMBERG BUSINESSWEEK, Mar. 19, 2015, *available at* https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies (last visited June 19, 2017).

[4] Joseph Menn, *Exclusive: Russian Antivirus Firm Faked Malware to Harm Rivals*, REUTERS, Aug. 14, 2015, *available at* www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QJ1CR20150814 (last visited June 27, 2017); *see also* Joseph Menn, *Exclusive: Russia's Kaspersky Threatened to 'Rub Out' Rival, Email Shows*, REUTERS, Aug. 28, 2015, *available at* http://www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QX2GO20150828 (last visited June 27, 2017).

[5] *Id.*

[6] *See* Ali Watkins, *US Officials Are Warning About A Russian Cybersecurity Company's US Government Ties*, BUZZFEED NEWS, May 8, 2017, *available at* https://www.buzzfeed.com/alimwatkins/us-officials-are-warning-about-a-russian-cybersecurity?utm_term=.osyYrP2Mz6#.kexPnOw1Lk (last visited June 19, 2017); *see also* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).

[7] Ken Dilanian & Tom Winter, *Bill Would Bar Pentagon From Business With Russian Cyber Firm Kaspersky*, NBC NEWS, June 28, 2017, *available at* http://www.nbcnews.com/news/us-news/fbi-interviews-employees-russia-linked-cyber-security-firm-kaspersky-lab-n777571 (last visited June 29, 2017); *see also* Joe Uchill, *FBI Visits Kaspersky Lab Employees*, THE HILL, June 28, 2017, *available at* http://thehill.com/policy/cybersecurity/339887-fbi-visits-kaspersky-lab-employees (last visited June 29, 2017).

[8] S. Comm. on Intel., *Worldwide Threats Hearing*, 115th Cong. (May 11, 2017). (question and answer by Senator Marco Rubio).

best practices for safeguarding against future cyber threats.[9] Among the panel of expert witnesses was Salim Neino, CEO of Kryptos Logic—the cybersecurity firm whose employee helped thwart further propagation of the recent WannaCry ransomware attack.[10] In response to questions about the ability of a software manufacturer to embed a "backdoor" into anti-virus software—to facilitate a State's cyber-espionage activities—Mr. Neino alarmingly affirmed that he had "seen that a multitude of times" in the past, and that the barriers to engaging in such activities are "very low."[11] This revelation gives the Committee great concern, especially in light of the capabilities that anti-virus software possesses. Additionally, in response to a question regarding Kaspersky Lab, retired Army General Gregory Touhill, the first federal chief information security officer or CISO, told the Committee: "I buy American."[12]

Anti-virus software is extremely powerful and operates by scanning files at the system level, rather than on the network periphery.[13] As such, other security systems generally do not monitor the operations carried out by the anti-virus software.[14] From a practical perspective, this means that compromised anti-virus software could be used for malicious or nefarious purposes, and could do so without detection. If anti-virus technology or systems are compromised by a user's adversary, it could install malicious code disguised as a security update; it could forego specific updates to pave the way for use of certain vectors of attack; it could forego beneficial updates for a specified subset of users; and it could even extract data that a user's adversary considers valuable.[15] Furthermore, anti-virus is so powerful that it has nearly unimpeded access into all attachments, files, and information contained on a system.[16] In sum, compromised anti-virus has the potential to undermine the security and integrity of any system on which it is installed.

The security and integrity of federal information systems are only as strong as the products that guard them. Although Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, requires federal departments and agencies to implement the NIST Cybersecurity Framework and to provide reports related thereto,[17] the

---

[9] H. Comm. on Science, Space, & Tech. Subcomm. on Research & Tech. jointly with the Subcomm. on Oversight, *Hearing on Bolstering the Government's Cybersecurity: Lessons Learned from WannaCry*, Preliminary Hearing Transcript, 115th Cong. (June 15, 2017) at 61.
[10] *Id.*
[11] *Id.* at 62 (question and answer by Representative Clay Higgins).
[12] *Id.* at 63.
[13] *See* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] The White House, *Executive Order – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017), *available at* https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal (last visited June 29, 2017).

security of federal systems may nevertheless be undermined by compromised anti-virus products. Government contracting data indicating that several federal departments and agencies use or have used cybersecurity or anti-virus products manufactured by Kaspersky Lab is even more troubling.[18] If federal agencies and departments are being guarded by potentially compromised software, then it is virtually impossible for such agencies to effectively and efficiently implement the NIST Framework, and to fully comply with President Trump's executive order. The recent news that Kaspersky Lab's products have been removed from the General Service Administration's contracting Schedule 67 and 70 is encouraging, however federal agencies and contractors may be likely to continue use of Kaspersky Lab's products.[19]

Cybersecurity is a greater threat to our nation than ever before. If these widely reported allegations prove true, then the American public has ample grounds on which to rest their concerns about the security of data stored and transmitted on federal information systems—especially those allegedly protected by Kaspersky Lab's products. In light of this increasing threat, the Committee takes seriously its duty to ensure the NIST Cybersecurity Framework is properly equipped and adapted to safeguard our nation's information. To assist the Committee in understanding the effectiveness of the NIST Framework, and potential vulnerabilities that exist on federal information systems, please provide the following documents and information as soon as possible, but no later than August 11, 2017. Please provide the requested materials for the time frame from January 1, 2013, to present:

1. All documents and communications referring or relating to cybersecurity and/or anti-virus products manufactured by Kaspersky Lab.

2. All documents and communications referring or relating to any evaluation, risk assessment, and decision-making processes on the matter of whether to implement products manufactured by Kaspersky Lab.

3. All documents and communications referring or relating to the use or implementation of products manufactured by Kaspersky Lab.

---

[18] Government Contracting Dataset, *available at* https://www.usaspending.gov/Pages/AdvancedSearch.aspx?k=kaspersky (last visited June 29, 2017); *see* David Goldstein & Greg Gordon, *Exclusive: Kremlin Documents Suggest Link Between Cyber Giant and Russia Spy Agency*, MCCLATCHY, July 3, 2017, *available at* http://www.mcclatchydc.com/news/nation-world/national/article159342694.html (last visited July 12, 2017); *see also* Mike Levine & Pierre Thomas, *Officials Fear Russia Could Try To Target US Through Popular Software Firm Under FBI Scrutiny*, ABC NEWS, May 9, 2017, *available at* http://abcnews.go.com/US/officials-fear-russia-target-us-popular-software-firm/story?id=47295729 (last visited July 12, 2017).

[19] *See* Sarah Kuranda, *Kaspersky Lab Removed From GSA Schedule, Limiting Federal Sales for Its Security Software*, CRN, July 12, 2017, *available at* http://www.crn.com/news/security/300088591/kaspersky-removed-from-gsa-schedule-limiting-federal-sales-for-its-security-software.htm; *see also* Eric Geller, *Trump Administration Restricts Popular Russian Security Software*, POLITICO, July 11, 2017, *available at* http://www.politico.com/story/2017/07/11/trump-russian-security-software-240423.

4. A complete list of any computers, systems, data, media, and/or information utilizing or accessible to Kaspersky Lab products or services.

5. Identify any federal government contractors or subcontractors known to be utilizing Kaspersky Lab's products to fulfill requirements of contracts with the Department or Agency.

6. All documents and communications referring or relating to the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity.

7. All documents and communications referring or relating to the production of reports required by Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.

Pursuant to House Rule X, the Committee on Science, Space, and Technology has jurisdiction over National Institute of Standards and Technology which develops cybersecurity standards and guidelines for the federal government and recommendations for the private sector.

When producing documents to the Committee, please deliver production sets to the Majority Staff in Room 2321 of the Rayburn House Office Building and the Minority Staff in Room 394 of the Ford House Office Building. The Committee prefers, if possible, to receive all documents in electronic format.

If you have any questions about this request, please contact Drew Colliatie or Tom Connally at 202-225-6371. Thank you for your attention to this matter.

Sincerely,

Lamar Smith
Chairman

cc: The Honorable Eddie Bernice Johnson, Ranking Minority Member

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6301
(202) 225-6371
www.science.house.gov

July 27, 2017

The Honorable Wilbur Ross
Secretary
U.S. Department of Commerce
1401 Constitution Avenue NW
Washington D.C. 20230

Dear Secretary Ross,

As part of an ongoing review of the federal government's cybersecurity policies and standards, the Committee on Science, Space, and Technology is requesting information and documents from the Department regarding Kaspersky Lab. The Committee is charged with oversight of the National Institute of Standards and Technology (NIST), and continuously evaluates whether changes to the Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework) are necessary. The documents and information will assist the Committee in determining whether the Framework requires further refinement when implemented by federal departments and agencies.

Kaspersky Lab is among the world's largest cybersecurity companies. Headquartered in Moscow, Russia, it services approximately 400 million users worldwide, including a number of United States Government Agencies and entities.[1] Kaspersky Lab specializes in anti-virus software—products with potentially uninhibited access to the systems they protect.[2] Although Kaspersky Lab was once considered a reputable cybersecurity firm, several concerns have been raised regarding the company and Eugene Kaspersky—the founder and CEO of Kaspersky Lab—and his potential ties to the Russian government.

The Committee is concerned that Kaspersky Lab is susceptible to manipulation by the Russian government, and that its products could be used as a tool for espionage, sabotage, or other nefarious activities against the United States. As early as 2015, reports began to surface

---

[1] *See* Jordan Robertson, *A Russian Cybersecurity Company's Ties to the Kremlin*, BLOOMBERG GOVERNMENT, Jul. 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSXAKB6JIJVL (last visited July 11, 2017).
[2] *See* Jordan Robertson & Michael Riley, *Kaspersky Lab Has Been Working With Russian Intelligence*, BLOOMBERG GOVERNMENT, July 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSX50G6KLVR5 (last visited July 11, 2017).

alleging that Mr. Kaspersky may have "close ties to Russian spies."[3] Shortly thereafter, *Reuters* reported that Kaspersky Lab engaged in a "sabotage" campaign undoubtedly targeting the U.S. cybersecurity market.[4] Specifically, the company "tried to damage rivals in the marketplace by tricking their antivirus software programs into classifying benign files as malicious."[5] More recently, Russia's alleged interference in the 2016 presidential election has heightened public concerns about the Kremlin's desire to meddle with American democratic processes. This, in turn, has ignited speculation over America's cybersecurity posture, and the potential ties that Kaspersky Lab has with the Kremlin. Namely, that the Russian government could use products manufactured by Kaspersky Lab as a medium for engaging in nefarious cyber campaigns against U.S. information systems—including those at several federal departments and agencies—that are purportedly protected by the company's products.[6] Adding to concern, the FBI sent agents to visit "at least a dozen employees of Kaspersky" in order to question them "about the company's operations as part of a counter-intelligence inquiry."[7]

Given the increasing prevalence of cybersecurity threats across the nation, the federal government's use of cybersecurity products manufactured by a firm with potential ties to the Russian government is concerning to Congress. In May, the Senate Intelligence Committee held an open hearing where several top U.S. intelligence officials stated with consensus that they would not be comfortable using Kaspersky Lab's products on their systems.[8] Additionally, on June 15, 2017, the House Science Committee Subcommittees on Oversight and Research and Technology held a joint hearing where cybersecurity experts testified on industry approaches and

---

[3] Carol Matlack, *The Company Securing Your Internet Has Close Ties to Russian Spies*, BLOOMBERG BUSINESSWEEK, Mar. 19, 2015, *available at* https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies (last visited June 19, 2017).

[4] Joseph Menn, *Exclusive: Russian Antivirus Firm Faked Malware to Harm Rivals*, REUTERS, Aug. 14, 2015, *available at* www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QJ1CR20150814 (last visited June 27, 2017); *see also* Joseph Menn, *Exclusive: Russia's Kaspersky Threatened to 'Rub Out' Rival, Email Shows*, REUTERS, Aug. 28, 2015, *available at* http://www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QX2GO20150828 (last visited June 27, 2017).

[5] *Id.*

[6] *See* Ali Watkins, *US Officials Are Warning About A Russian Cybersecurity Company's US Government Ties*, BUZZFEED NEWS, May 8, 2017, *available at* https://www.buzzfeed.com/alimwatkins/us-officials-are-warning-about-a-russian-cybersecurity?utm_term=.osyYrP2Mz6#.kexPnOw1Lk (last visited June 19, 2017); *see also* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).

[7] Ken Dilanian & Tom Winter, *Bill Would Bar Pentagon From Business With Russian Cyber Firm Kaspersky*, NBC NEWS, June 28, 2017, *available at* http://www.nbcnews.com/news/us-news/fbi-interviews-employees-russia-linked-cyber-security-firm-kaspersky-lab-n777571 (last visited June 29, 2017); *see also* Joe Uchill, *FBI Visits Kaspersky Lab Employees*, THE HILL, June 28, 2017, *available at* http://thehill.com/policy/cybersecurity/339887-fbi-visits-kaspersky-lab-employees (last visited June 29, 2017).

[8] S. Comm. on Intel., *Worldwide Threats Hearing*, 115th Cong. (May 11, 2017). (question and answer by Senator Marco Rubio).

best practices for safeguarding against future cyber threats.[9] Among the panel of expert witnesses was Salim Neino, CEO of Kryptos Logic—the cybersecurity firm whose employee helped thwart further propagation of the recent WannaCry ransomware attack.[10] In response to questions about the ability of a software manufacturer to embed a "backdoor" into anti-virus software—to facilitate a State's cyber-espionage activities—Mr. Neino alarmingly affirmed that he had "seen that a multitude of times" in the past, and that the barriers to engaging in such activities are "very low."[11] This revelation gives the Committee great concern, especially in light of the capabilities that anti-virus software possesses. Additionally, in response to a question regarding Kaspersky Lab, retired Army General Gregory Touhill, the first federal chief information security officer or CISO, told the Committee: "I buy American."[12]

Anti-virus software is extremely powerful and operates by scanning files at the system level, rather than on the network periphery.[13] As such, other security systems generally do not monitor the operations carried out by the anti-virus software.[14] From a practical perspective, this means that compromised anti-virus software could be used for malicious or nefarious purposes, and could do so without detection. If anti-virus technology or systems are compromised by a user's adversary, it could install malicious code disguised as a security update; it could forego specific updates to pave the way for use of certain vectors of attack; it could forego beneficial updates for a specified subset of users; and it could even extract data that a user's adversary considers valuable.[15] Furthermore, anti-virus is so powerful that it has nearly unimpeded access into all attachments, files, and information contained on a system.[16] In sum, compromised anti-virus has the potential to undermine the security and integrity of any system on which it is installed.

The security and integrity of federal information systems are only as strong as the products that guard them. Although Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, requires federal departments and agencies to implement the NIST Cybersecurity Framework and to provide reports related thereto,[17] the

---

[9] H. Comm. on Science, Space, & Tech. Subcomm. on Research & Tech. jointly with the Subcomm. on Oversight, *Hearing on Bolstering the Government's Cybersecurity: Lessons Learned from WannaCry*, Preliminary Hearing Transcript, 115th Cong. (June 15, 2017) at 61.

[10] *Id.*

[11] *Id.* at 62 (question and answer by Representative Clay Higgins).

[12] *Id.* at 63.

[13] *See* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).

[14] *Id.*

[15] *Id.*

[16] *Id.*

[17] The White House, *Executive Order – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017), *available at* https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal (last visited June 29, 2017).

security of federal systems may nevertheless be undermined by compromised anti-virus products. Government contracting data indicating that several federal departments and agencies use or have used cybersecurity or anti-virus products manufactured by Kaspersky Lab is even more troubling.[18] If federal agencies and departments are being guarded by potentially compromised software, then it is virtually impossible for such agencies to effectively and efficiently implement the NIST Framework, and to fully comply with President Trump's executive order. The recent news that Kaspersky Lab's products have been removed from the General Service Administration's contracting Schedule 67 and 70 is encouraging, however federal agencies and contractors may be likely to continue use of Kaspersky Lab's products.[19]

Cybersecurity is a greater threat to our nation than ever before. If these widely reported allegations prove true, then the American public has ample grounds on which to rest their concerns about the security of data stored and transmitted on federal information systems—especially those allegedly protected by Kaspersky Lab's products. In light of this increasing threat, the Committee takes seriously its duty to ensure the NIST Cybersecurity Framework is properly equipped and adapted to safeguard our nation's information. To assist the Committee in understanding the effectiveness of the NIST Framework, and potential vulnerabilities that exist on federal information systems, please provide the following documents and information as soon as possible, but no later than August 11, 2017. Please provide the requested materials for the time frame from January 1, 2013, to present:

1. All documents and communications referring or relating to cybersecurity and/or anti-virus products manufactured by Kaspersky Lab.

2. All documents and communications referring or relating to any evaluation, risk assessment, and decision-making processes on the matter of whether to implement products manufactured by Kaspersky Lab.

3. All documents and communications referring or relating to the use or implementation of products manufactured by Kaspersky Lab.

---

[18] Government Contracting Dataset, *available at* https://www.usaspending.gov/Pages/AdvancedSearch.aspx?k=kaspersky (last visited June 29, 2017); *see* David Goldstein & Greg Gordon, *Exclusive: Kremlin Documents Suggest Link Between Cyber Giant and Russia Spy Agency*, MCCLATCHY, July 3, 2017, *available at* http://www.mcclatchydc.com/news/nation-world/national/article159342694.html (last visited July 12, 2017); *see also* Mike Levine & Pierre Thomas, *Officials Fear Russia Could Try To Target US Through Popular Software Firm Under FBI Scrutiny*, ABC NEWS, May 9, 2017, *available at* http://abcnews.go.com/US/officials-fear-russia-target-us-popular-software-firm/story?id=47295729 (last visited July 12, 2017).

[19] *See* Sarah Kuranda, *Kaspersky Lab Removed From GSA Schedule, Limiting Federal Sales for Its Security Software*, CRN, July 12, 2017, *available at* http://www.crn.com/news/security/300088591/kaspersky-removed-from-gsa-schedule-limiting-federal-sales-for-its-security-software.htm; *see also* Eric Geller, *Trump Administration Restricts Popular Russian Security Software*, POLITICO, July 11, 2017, *available at* http://www.politico.com/story/2017/07/11/trump-russian-security-software-240423.

4. A complete list of any computers, systems, data, media, and/or information utilizing or accessible to Kaspersky Lab products or services.

5. Identify any federal government contractors or subcontractors known to be utilizing Kaspersky Lab's products to fulfill requirements of contracts with the Department or Agency.

6. All documents and communications referring or relating to the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity.

7. All documents and communications referring or relating to the production of reports required by Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.

Pursuant to House Rule X, the Committee on Science, Space, and Technology has jurisdiction over National Institute of Standards and Technology which develops cybersecurity standards and guidelines for the federal government and recommendations for the private sector.

When producing documents to the Committee, please deliver production sets to the Majority Staff in Room 2321 of the Rayburn House Office Building and the Minority Staff in Room 394 of the Ford House Office Building. The Committee prefers, if possible, to receive all documents in electronic format.

If you have any questions about this request, please contact Drew Colliatie or Tom Connally at 202-225-6371. Thank you for your attention to this matter.

Sincerely,

Lamar Smith
Chairman

cc: The Honorable Eddie Bernice Johnson, Ranking Minority Member

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6301
(202) 225–6371
www.science.house.gov

July 27, 2017

The Honorable Ann Marie Buerkle
Acting Chairman
U.S. Consumer Product Safety Commission
4330 East West Highway
Bethesda, MD 20814

Dear Acting Chairman Buerkle,

As part of an ongoing review of the federal government's cybersecurity policies and standards, the Committee on Science, Space, and Technology is requesting information and documents from the Commission regarding Kaspersky Lab. The Committee is charged with oversight of the National Institute of Standards and Technology (NIST), and continuously evaluates whether changes to the Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework) are necessary. The documents and information will assist the Committee in determining whether the Framework requires further refinement when implemented by federal departments and agencies.

Kaspersky Lab is among the world's largest cybersecurity companies. Headquartered in Moscow, Russia, it services approximately 400 million users worldwide, including a number of United States Government Agencies and entities.[1] Kaspersky Lab specializes in anti-virus software—products with potentially uninhibited access to the systems they protect.[2] Although Kaspersky Lab was once considered a reputable cybersecurity firm, several concerns have been raised regarding the company and Eugene Kaspersky—the founder and CEO of Kaspersky Lab—and his potential ties to the Russian government.

The Committee is concerned that Kaspersky Lab is susceptible to manipulation by the Russian government, and that its products could be used as a tool for espionage, sabotage, or other nefarious activities against the United States. As early as 2015, reports began to surface

---

[1] *See* Jordan Robertson, *A Russian Cybersecurity Company's Ties to the Kremlin*, BLOOMBERG GOVERNMENT, Jul. 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSXAKB6JIJVL (last visited July 11, 2017).
[2] *See* Jordan Robertson & Michael Riley, *Kaspersky Lab Has Been Working With Russian Intelligence*, BLOOMBERG GOVERNMENT, July 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSX50G6KLVR5 (last visited July 11, 2017).

alleging that Mr. Kaspersky may have "close ties to Russian spies."[3] Shortly thereafter, *Reuters* reported that Kaspersky Lab engaged in a "sabotage" campaign undoubtedly targeting the U.S. cybersecurity market.[4] Specifically, the company "tried to damage rivals in the marketplace by tricking their antivirus software programs into classifying benign files as malicious."[5] More recently, Russia's alleged interference in the 2016 presidential election has heightened public concerns about the Kremlin's desire to meddle with American democratic processes. This, in turn, has ignited speculation over America's cybersecurity posture, and the potential ties that Kaspersky Lab has with the Kremlin. Namely, that the Russian government could use products manufactured by Kaspersky Lab as a medium for engaging in nefarious cyber campaigns against U.S. information systems—including those at several federal departments and agencies—that are purportedly protected by the company's products.[6] Adding to concern, the FBI sent agents to visit "at least a dozen employees of Kaspersky" in order to question them "about the company's operations as part of a counter-intelligence inquiry."[7]

Given the increasing prevalence of cybersecurity threats across the nation, the federal government's use of cybersecurity products manufactured by a firm with potential ties to the Russian government is concerning to Congress. In May, the Senate Intelligence Committee held an open hearing where several top U.S. intelligence officials stated with consensus that they would not be comfortable using Kaspersky Lab's products on their systems.[8] Additionally, on June 15, 2017, the House Science Committee Subcommittees on Oversight and Research and Technology held a joint hearing where cybersecurity experts testified on industry approaches and

---

[3] Carol Matlack, *The Company Securing Your Internet Has Close Ties to Russian Spies*, BLOOMBERG BUSINESSWEEK, Mar. 19, 2015, *available at* https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies (last visited June 19, 2017).

[4] Joseph Menn, *Exclusive: Russian Antivirus Firm Faked Malware to Harm Rivals*, REUTERS, Aug. 14, 2015, *available at* www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QJ1CR20150814 (last visited June 27, 2017); *see also* Joseph Menn, *Exclusive: Russia's Kaspersky Threatened to 'Rub Out' Rival, Email Shows*, REUTERS, Aug. 28, 2015, *available at* http://www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QX2GO20150828 (last visited June 27, 2017).

[5] *Id.*

[6] *See* Ali Watkins, *US Officials Are Warning About A Russian Cybersecurity Company's US Government Ties*, BUZZFEED NEWS, May 8, 2017, *available at* https://www.buzzfeed.com/alimwatkins/us-officials-are-warning-about-a-russian-cybersecurity?utm_term=.osyYrP2Mz6#.kexPnOw1Lk (last visited June 19, 2017); *see also* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).

[7] Ken Dilanian & Tom Winter, *Bill Would Bar Pentagon From Business With Russian Cyber Firm Kaspersky*, NBC NEWS, June 28, 2017, *available at* http://www.nbcnews.com/news/us-news/fbi-interviews-employees-russia-linked-cyber-security-firm-kaspersky-lab-n777571 (last visited June 29, 2017); *see also* Joe Uchill, *FBI Visits Kaspersky Lab Employees*, THE HILL, June 28, 2017, *available at* http://thehill.com/policy/cybersecurity/339887-fbi-visits-kaspersky-lab-employees (last visited June 29, 2017).

[8] S. Comm. on Intel., *Worldwide Threats Hearing*, 115th Cong. (May 11, 2017). (question and answer by Senator Marco Rubio).

best practices for safeguarding against future cyber threats.[9] Among the panel of expert witnesses was Salim Neino, CEO of Kryptos Logic—the cybersecurity firm whose employee helped thwart further propagation of the recent WannaCry ransomware attack.[10] In response to questions about the ability of a software manufacturer to embed a "backdoor" into anti-virus software—to facilitate a State's cyber-espionage activities—Mr. Neino alarmingly affirmed that he had "seen that a multitude of times" in the past, and that the barriers to engaging in such activities are "very low."[11] This revelation gives the Committee great concern, especially in light of the capabilities that anti-virus software possesses. Additionally, in response to a question regarding Kaspersky Lab, retired Army General Gregory Touhill, the first federal chief information security officer or CISO, told the Committee: "I buy American."[12]

Anti-virus software is extremely powerful and operates by scanning files at the system level, rather than on the network periphery.[13] As such, other security systems generally do not monitor the operations carried out by the anti-virus software.[14] From a practical perspective, this means that compromised anti-virus software could be used for malicious or nefarious purposes, and could do so without detection. If anti-virus technology or systems are compromised by a user's adversary, it could install malicious code disguised as a security update; it could forego specific updates to pave the way for use of certain vectors of attack; it could forego beneficial updates for a specified subset of users; and it could even extract data that a user's adversary considers valuable.[15] Furthermore, anti-virus is so powerful that it has nearly unimpeded access into all attachments, files, and information contained on a system.[16] In sum, compromised anti-virus has the potential to undermine the security and integrity of any system on which it is installed.

The security and integrity of federal information systems are only as strong as the products that guard them. Although Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, requires federal departments and agencies to implement the NIST Cybersecurity Framework and to provide reports related thereto,[17] the

---

[9] H. Comm. on Science, Space, & Tech. Subcomm. on Research & Tech. jointly with the Subcomm. on Oversight, *Hearing on Bolstering the Government's Cybersecurity: Lessons Learned from WannaCry*, Preliminary Hearing Transcript, 115th Cong. (June 15, 2017) at 61.
[10] *Id.*
[11] *Id.* at 62 (question and answer by Representative Clay Higgins).
[12] *Id.* at 63.
[13] *See* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] The White House, *Executive Order – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017), *available at* https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal (last visited June 29, 2017).

security of federal systems may nevertheless be undermined by compromised anti-virus products. Government contracting data indicating that several federal departments and agencies use or have used cybersecurity or anti-virus products manufactured by Kaspersky Lab is even more troubling.[18] If federal agencies and departments are being guarded by potentially compromised software, then it is virtually impossible for such agencies to effectively and efficiently implement the NIST Framework, and to fully comply with President Trump's executive order. The recent news that Kaspersky Lab's products have been removed from the General Service Administration's contracting Schedule 67 and 70 is encouraging, however federal agencies and contractors may be likely to continue use of Kaspersky Lab's products.[19]

Cybersecurity is a greater threat to our nation than ever before. If these widely reported allegations prove true, then the American public has ample grounds on which to rest their concerns about the security of data stored and transmitted on federal information systems—especially those allegedly protected by Kaspersky Lab's products. In light of this increasing threat, the Committee takes seriously its duty to ensure the NIST Cybersecurity Framework is properly equipped and adapted to safeguard our nation's information. To assist the Committee in understanding the effectiveness of the NIST Framework, and potential vulnerabilities that exist on federal information systems, please provide the following documents and information as soon as possible, but no later than August 11, 2017. Please provide the requested materials for the time frame from January 1, 2013, to present:

1. All documents and communications referring or relating to cybersecurity and/or anti-virus products manufactured by Kaspersky Lab.

2. All documents and communications referring or relating to any evaluation, risk assessment, and decision-making processes on the matter of whether to implement products manufactured by Kaspersky Lab.

3. All documents and communications referring or relating to the use or implementation of products manufactured by Kaspersky Lab.

---

[18] Government Contracting Dataset, *available at* https://www.usaspending.gov/Pages/AdvancedSearch.aspx?k=kaspersky (last visited June 29, 2017); *see* David Goldstein & Greg Gordon, *Exclusive: Kremlin Documents Suggest Link Between Cyber Giant and Russia Spy Agency*, MCCLATCHY, July 3, 2017, *available at* http://www.mcclatchydc.com/news/nation-world/national/article159342694.html (last visited July 12, 2017); *see also* Mike Levine & Pierre Thomas, *Officials Fear Russia Could Try To Target US Through Popular Software Firm Under FBI Scrutiny*, ABC NEWS, May 9, 2017, *available at* http://abcnews.go.com/US/officials-fear-russia-target-us-popular-software-firm/story?id=47295729 (last visited July 12, 2017).

[19] *See* Sarah Kuranda, *Kaspersky Lab Removed From GSA Schedule, Limiting Federal Sales for Its Security Software*, CRN, July 12, 2017, *available at* http://www.crn.com/news/security/300088591/kaspersky-removed-from-gsa-schedule-limiting-federal-sales-for-its-security-software.htm; *see also* Eric Geller, *Trump Administration Restricts Popular Russian Security Software*, POLITICO, July 11, 2017, *available at* http://www.politico.com/story/2017/07/11/trump-russian-security-software-240423.

4. A complete list of any computers, systems, data, media, and/or information utilizing or accessible to Kaspersky Lab products or services.

5. Identify any federal government contractors or subcontractors known to be utilizing Kaspersky Lab's products to fulfill requirements of contracts with the Department or Agency.

6. All documents and communications referring or relating to the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity.

7. All documents and communications referring or relating to the production of reports required by Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.

Pursuant to House Rule X, the Committee on Science, Space, and Technology has jurisdiction over National Institute of Standards and Technology which develops cybersecurity standards and guidelines for the federal government and recommendations for the private sector.

When producing documents to the Committee, please deliver production sets to the Majority Staff in Room 2321 of the Rayburn House Office Building and the Minority Staff in Room 394 of the Ford House Office Building. The Committee prefers, if possible, to receive all documents in electronic format.

If you have any questions about this request, please contact Drew Colliatie or Tom Connally at 202-225-6371. Thank you for your attention to this matter.

Sincerely,

Lamar Smith
Chairman

cc: The Honorable Eddie Bernice Johnson, Ranking Minority Member

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6301
(202) 225–6371
www.science.house.gov

July 27, 2017

The Honorable John F. Kelly
Secretary
U.S. Department of Homeland Security
3801 Nebraska Avenue NW
Washington D.C. 20016 - 3621

Dear Secretary Kelly,

As part of an ongoing review of the federal government's cybersecurity policies and standards, the Committee on Science, Space, and Technology is requesting information and documents from the Department regarding Kaspersky Lab. The Committee is charged with oversight of the National Institute of Standards and Technology (NIST), and continuously evaluates whether changes to the Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework) are necessary. The documents and information will assist the Committee in determining whether the Framework requires further refinement when implemented by federal departments and agencies.

Kaspersky Lab is among the world's largest cybersecurity companies. Headquartered in Moscow, Russia, it services approximately 400 million users worldwide, including a number of United States Government Agencies and entities.[1] Kaspersky Lab specializes in anti-virus software—products with potentially uninhibited access to the systems they protect.[2] Although Kaspersky Lab was once considered a reputable cybersecurity firm, several concerns have been raised regarding the company and Eugene Kaspersky—the founder and CEO of Kaspersky Lab—and his potential ties to the Russian government.

The Committee is concerned that Kaspersky Lab is susceptible to manipulation by the Russian government, and that its products could be used as a tool for espionage, sabotage, or other nefarious activities against the United States. As early as 2015, reports began to surface

---

[1] *See* Jordan Robertson, *A Russian Cybersecurity Company's Ties to the Kremlin*, BLOOMBERG GOVERNMENT, Jul. 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSXAKB6JIJVL (last visited July 11, 2017).
[2] *See* Jordan Robertson & Michael Riley, *Kaspersky Lab Has Been Working With Russian Intelligence*, BLOOMBERG GOVERNMENT, July 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSX50G6KLVR5 (last visited July 11, 2017).

alleging that Mr. Kaspersky may have "close ties to Russian spies."[3] Shortly thereafter, *Reuters* reported that Kaspersky Lab engaged in a "sabotage" campaign undoubtedly targeting the U.S. cybersecurity market.[4] Specifically, the company "tried to damage rivals in the marketplace by tricking their antivirus software programs into classifying benign files as malicious."[5] More recently, Russia's alleged interference in the 2016 presidential election has heightened public concerns about the Kremlin's desire to meddle with American democratic processes. This, in turn, has ignited speculation over America's cybersecurity posture, and the potential ties that Kaspersky Lab has with the Kremlin. Namely, that the Russian government could use products manufactured by Kaspersky Lab as a medium for engaging in nefarious cyber campaigns against U.S. information systems—including those at several federal departments and agencies—that are purportedly protected by the company's products.[6] Adding to concern, the FBI sent agents to visit "at least a dozen employees of Kaspersky" in order to question them "about the company's operations as part of a counter-intelligence inquiry."[7]

Given the increasing prevalence of cybersecurity threats across the nation, the federal government's use of cybersecurity products manufactured by a firm with potential ties to the Russian government is concerning to Congress. In May, the Senate Intelligence Committee held an open hearing where several top U.S. intelligence officials stated with consensus that they would not be comfortable using Kaspersky Lab's products on their systems.[8] Additionally, on June 15, 2017, the House Science Committee Subcommittees on Oversight and Research and Technology held a joint hearing where cybersecurity experts testified on industry approaches and

---

[3] Carol Matlack, *The Company Securing Your Internet Has Close Ties to Russian Spies*, BLOOMBERG BUSINESSWEEK, Mar. 19, 2015, *available at* https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies (last visited June 19, 2017).

[4] Joseph Menn, *Exclusive: Russian Antivirus Firm Faked Malware to Harm Rivals*, REUTERS, Aug. 14, 2015, *available at* www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QJ1CR20150814 (last visited June 27, 2017); *see also* Joseph Menn, *Exclusive: Russia's Kaspersky Threatened to 'Rub Out' Rival, Email Shows*, REUTERS, Aug. 28, 2015, *available at* http://www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QX2GO20150828 (last visited June 27, 2017).

[5] *Id.*

[6] *See* Ali Watkins, *US Officials Are Warning About A Russian Cybersecurity Company's US Government Ties*, BUZZFEED NEWS, May 8, 2017, *available at* https://www.buzzfeed.com/alimwatkins/us-officials-are-warning-about-a-russian-cybersecurity?utm_term=.osyYrP2Mz6#.kexPnOw1Lk (last visited June 19, 2017); *see also* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).

[7] Ken Dilanian & Tom Winter, *Bill Would Bar Pentagon From Business With Russian Cyber Firm Kaspersky*, NBC NEWS, June 28, 2017, *available at* http://www.nbcnews.com/news/us-news/fbi-interviews-employees-russia-linked-cyber-security-firm-kaspersky-lab-n777571 (last visited June 29, 2017); *see also* Joe Uchill, *FBI Visits Kaspersky Lab Employees*, THE HILL, June 28, 2017, *available at* http://thehill.com/policy/cybersecurity/339887-fbi-visits-kaspersky-lab-employees (last visited June 29, 2017).

[8] S. Comm. on Intel., *Worldwide Threats Hearing*, 115th Cong. (May 11, 2017). (question and answer by Senator Marco Rubio).

best practices for safeguarding against future cyber threats.[9] Among the panel of expert witnesses was Salim Neino, CEO of Kryptos Logic—the cybersecurity firm whose employee helped thwart further propagation of the recent WannaCry ransomware attack.[10] In response to questions about the ability of a software manufacturer to embed a "backdoor" into anti-virus software—to facilitate a State's cyber-espionage activities—Mr. Neino alarmingly affirmed that he had "seen that a multitude of times" in the past, and that the barriers to engaging in such activities are "very low."[11] This revelation gives the Committee great concern, especially in light of the capabilities that anti-virus software possesses. Additionally, in response to a question regarding Kaspersky Lab, retired Army General Gregory Touhill, the first federal chief information security officer or CISO, told the Committee: "I buy American."[12]

Anti-virus software is extremely powerful and operates by scanning files at the system level, rather than on the network periphery.[13] As such, other security systems generally do not monitor the operations carried out by the anti-virus software.[14] From a practical perspective, this means that compromised anti-virus software could be used for malicious or nefarious purposes, and could do so without detection. If anti-virus technology or systems are compromised by a user's adversary, it could install malicious code disguised as a security update; it could forego specific updates to pave the way for use of certain vectors of attack; it could forego beneficial updates for a specified subset of users; and it could even extract data that a user's adversary considers valuable.[15] Furthermore, anti-virus is so powerful that it has nearly unimpeded access into all attachments, files, and information contained on a system.[16] In sum, compromised anti-virus has the potential to undermine the security and integrity of any system on which it is installed.

The security and integrity of federal information systems are only as strong as the products that guard them. Although Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, requires federal departments and agencies to implement the NIST Cybersecurity Framework and to provide reports related thereto,[17] the

---

[9] H. Comm. on Science, Space, & Tech. Subcomm. on Research & Tech. jointly with the Subcomm. on Oversight, *Hearing on Bolstering the Government's Cybersecurity: Lessons Learned from WannaCry*, Preliminary Hearing Transcript, 115th Cong. (June 15, 2017) at 61.
[10] *Id.*
[11] *Id.* at 62 (question and answer by Representative Clay Higgins).
[12] *Id.* at 63.
[13] *See* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] The White House, *Executive Order – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017), *available at* https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal (last visited June 29, 2017).

security of federal systems may nevertheless be undermined by compromised anti-virus products. Government contracting data indicating that several federal departments and agencies use or have used cybersecurity or anti-virus products manufactured by Kaspersky Lab is even more troubling.[18] If federal agencies and departments are being guarded by potentially compromised software, then it is virtually impossible for such agencies to effectively and efficiently implement the NIST Framework, and to fully comply with President Trump's executive order. The recent news that Kaspersky Lab's products have been removed from the General Service Administration's contracting Schedule 67 and 70 is encouraging, however federal agencies and contractors may be likely to continue use of Kaspersky Lab's products.[19]

Cybersecurity is a greater threat to our nation than ever before. If these widely reported allegations prove true, then the American public has ample grounds on which to rest their concerns about the security of data stored and transmitted on federal information systems—especially those allegedly protected by Kaspersky Lab's products. In light of this increasing threat, the Committee takes seriously its duty to ensure the NIST Cybersecurity Framework is properly equipped and adapted to safeguard our nation's information. To assist the Committee in understanding the effectiveness of the NIST Framework, and potential vulnerabilities that exist on federal information systems, please provide the following documents and information as soon as possible, but no later than August 11, 2017. Please provide the requested materials for the time frame from January 1, 2013, to present:

1. All documents and communications referring or relating to cybersecurity and/or anti-virus products manufactured by Kaspersky Lab.

2. All documents and communications referring or relating to any evaluation, risk assessment, and decision-making processes on the matter of whether to implement products manufactured by Kaspersky Lab.

3. All documents and communications referring or relating to the use or implementation of products manufactured by Kaspersky Lab.

---

[18] Government Contracting Dataset, *available at* https://www.usaspending.gov/Pages/AdvancedSearch.aspx?k=kaspersky (last visited June 29, 2017); *see* David Goldstein & Greg Gordon, *Exclusive: Kremlin Documents Suggest Link Between Cyber Giant and Russia Spy Agency*, MCCLATCHY, July 3, 2017, *available at* http://www.mcclatchydc.com/news/nation-world/national/article159342694.html (last visited July 12, 2017); *see also* Mike Levine & Pierre Thomas, *Officials Fear Russia Could Try To Target US Through Popular Software Firm Under FBI Scrutiny*, ABC NEWS, May 9, 2017, *available at* http://abcnews.go.com/US/officials-fear-russia-target-us-popular-software-firm/story?id=47295729 (last visited July 12, 2017).

[19] *See* Sarah Kuranda, *Kaspersky Lab Removed From GSA Schedule, Limiting Federal Sales for Its Security Software*, CRN, July 12, 2017, *available at* http://www.crn.com/news/security/300088591/kaspersky-removed-from-gsa-schedule-limiting-federal-sales-for-its-security-software.htm; *see also* Eric Geller, *Trump Administration Restricts Popular Russian Security Software*, POLITICO, July 11, 2017, *available at* http://www.politico.com/story/2017/07/11/trump-russian-security-software-240423.

4. A complete list of any computers, systems, data, media, and/or information utilizing or accessible to Kaspersky Lab products or services.

5. Identify any federal government contractors or subcontractors known to be utilizing Kaspersky Lab's products to fulfill requirements of contracts with the Department or Agency.

6. All documents and communications referring or relating to the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity.

7. All documents and communications referring or relating to the production of reports required by Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.

Pursuant to House Rule X, the Committee on Science, Space, and Technology has jurisdiction over National Institute of Standards and Technology which develops cybersecurity standards and guidelines for the federal government and recommendations for the private sector.

When producing documents to the Committee, please deliver production sets to the Majority Staff in Room 2321 of the Rayburn House Office Building and the Minority Staff in Room 394 of the Ford House Office Building. The Committee prefers, if possible, to receive all documents in electronic format.

If you have any questions about this request, please contact Drew Colliatie or Tom Connally at 202-225-6371. Thank you for your attention to this matter.

Sincerely,

Lamar Smith

Lamar Smith
Chairman

cc: The Honorable Eddie Bernice Johnson, Ranking Minority Member

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6301
(202) 225–6371
www.science.house.gov

July 27, 2017

The Honorable James Mattis
Secretary
U.S. Department of Defense
1400 Defense Pentagon
Washington D.C. 20301 - 1400

Dear Secretary Mattis,

As part of an ongoing review of the federal government's cybersecurity policies and standards, the Committee on Science, Space, and Technology is requesting information and documents from the Department regarding Kaspersky Lab. The Committee is charged with oversight of the National Institute of Standards and Technology (NIST), and continuously evaluates whether changes to the Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework) are necessary. The documents and information will assist the Committee in determining whether the Framework requires further refinement when implemented by federal departments and agencies.

Kaspersky Lab is among the world's largest cybersecurity companies. Headquartered in Moscow, Russia, it services approximately 400 million users worldwide, including a number of United States Government Agencies and entities.[1] Kaspersky Lab specializes in anti-virus software—products with potentially uninhibited access to the systems they protect.[2] Although Kaspersky Lab was once considered a reputable cybersecurity firm, several concerns have been raised regarding the company and Eugene Kaspersky—the founder and CEO of Kaspersky Lab—and his potential ties to the Russian government.

The Committee is concerned that Kaspersky Lab is susceptible to manipulation by the Russian government, and that its products could be used as a tool for espionage, sabotage, or other nefarious activities against the United States. As early as 2015, reports began to surface

---

[1] *See* Jordan Robertson, *A Russian Cybersecurity Company's Ties to the Kremlin*, BLOOMBERG GOVERNMENT, Jul. 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSXAKB6JIJVL (last visited July 11, 2017).
[2] *See* Jordan Robertson & Michael Riley, *Kaspersky Lab Has Been Working With Russian Intelligence*, BLOOMBERG GOVERNMENT, July 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSX50G6KLVR5 (last visited July 11, 2017).

alleging that Mr. Kaspersky may have "close ties to Russian spies."[3] Shortly thereafter, *Reuters* reported that Kaspersky Lab engaged in a "sabotage" campaign undoubtedly targeting the U.S. cybersecurity market.[4] Specifically, the company "tried to damage rivals in the marketplace by tricking their antivirus software programs into classifying benign files as malicious."[5] More recently, Russia's alleged interference in the 2016 presidential election has heightened public concerns about the Kremlin's desire to meddle with American democratic processes. This, in turn, has ignited speculation over America's cybersecurity posture, and the potential ties that Kaspersky Lab has with the Kremlin. Namely, that the Russian government could use products manufactured by Kaspersky Lab as a medium for engaging in nefarious cyber campaigns against U.S. information systems—including those at several federal departments and agencies—that are purportedly protected by the company's products.[6] Adding to concern, the FBI sent agents to visit "at least a dozen employees of Kaspersky" in order to question them "about the company's operations as part of a counter-intelligence inquiry."[7]

Given the increasing prevalence of cybersecurity threats across the nation, the federal government's use of cybersecurity products manufactured by a firm with potential ties to the Russian government is concerning to Congress. In May, the Senate Intelligence Committee held an open hearing where several top U.S. intelligence officials stated with consensus that they would not be comfortable using Kaspersky Lab's products on their systems.[8] Additionally, on June 15, 2017, the House Science Committee Subcommittees on Oversight and Research and Technology held a joint hearing where cybersecurity experts testified on industry approaches and

---

[3] Carol Matlack, *The Company Securing Your Internet Has Close Ties to Russian Spies*, BLOOMBERG BUSINESSWEEK, Mar. 19, 2015, *available at* https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies (last visited June 19, 2017).

[4] Joseph Menn, *Exclusive: Russian Antivirus Firm Faked Malware to Harm Rivals*, REUTERS, Aug. 14, 2015, *available at* www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QJ1CR20150814 (last visited June 27, 2017); *see also* Joseph Menn, *Exclusive: Russia's Kaspersky Threatened to 'Rub Out' Rival, Email Shows*, REUTERS, Aug. 28, 2015, *available at* http://www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QX2GO20150828 (last visited June 27, 2017).

[5] *Id.*

[6] *See* Ali Watkins, *US Officials Are Warning About A Russian Cybersecurity Company's US Government Ties*, BUZZFEED NEWS, May 8, 2017, *available at* https://www.buzzfeed.com/alimwatkins/us-officials-are-warning-about-a-russian-cybersecurity?utm_term=.osyYrP2Mz6#.kexPnOw1Lk (last visited June 19, 2017); *see also* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).

[7] Ken Dilanian & Tom Winter, *Bill Would Bar Pentagon From Business With Russian Cyber Firm Kaspersky*, NBC NEWS, June 28, 2017, *available at* http://www.nbcnews.com/news/us-news/fbi-interviews-employees-russia-linked-cyber-security-firm-kaspersky-lab-n777571 (last visited June 29, 2017); *see also* Joe Uchill, *FBI Visits Kaspersky Lab Employees*, THE HILL, June 28, 2017, *available at* http://thehill.com/policy/cybersecurity/339887-fbi-visits-kaspersky-lab-employees (last visited June 29, 2017).

[8] S. Comm. on Intel., *Worldwide Threats Hearing*, 115th Cong. (May 11, 2017). (question and answer by Senator Marco Rubio).

best practices for safeguarding against future cyber threats.[9] Among the panel of expert witnesses was Salim Neino, CEO of Kryptos Logic—the cybersecurity firm whose employee helped thwart further propagation of the recent WannaCry ransomware attack.[10] In response to questions about the ability of a software manufacturer to embed a "backdoor" into anti-virus software—to facilitate a State's cyber-espionage activities—Mr. Neino alarmingly affirmed that he had "seen that a multitude of times" in the past, and that the barriers to engaging in such activities are "very low."[11] This revelation gives the Committee great concern, especially in light of the capabilities that anti-virus software possesses. Additionally, in response to a question regarding Kaspersky Lab, retired Army General Gregory Touhill, the first federal chief information security officer or CISO, told the Committee: "I buy American."[12]

Anti-virus software is extremely powerful and operates by scanning files at the system level, rather than on the network periphery.[13] As such, other security systems generally do not monitor the operations carried out by the anti-virus software.[14] From a practical perspective, this means that compromised anti-virus software could be used for malicious or nefarious purposes, and could do so without detection. If anti-virus technology or systems are compromised by a user's adversary, it could install malicious code disguised as a security update; it could forego specific updates to pave the way for use of certain vectors of attack; it could forego beneficial updates for a specified subset of users; and it could even extract data that a user's adversary considers valuable.[15] Furthermore, anti-virus is so powerful that it has nearly unimpeded access into all attachments, files, and information contained on a system.[16] In sum, compromised anti-virus has the potential to undermine the security and integrity of any system on which it is installed.

The security and integrity of federal information systems are only as strong as the products that guard them. Although Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, requires federal departments and agencies to implement the NIST Cybersecurity Framework and to provide reports related thereto,[17] the

---

[9] H. Comm. on Science, Space, & Tech. Subcomm. on Research & Tech. jointly with the Subcomm. on Oversight, *Hearing on Bolstering the Government's Cybersecurity: Lessons Learned from WannaCry*, Preliminary Hearing Transcript, 115th Cong. (June 15, 2017) at 61.
[10] *Id.*
[11] *Id.* at 62 (question and answer by Representative Clay Higgins).
[12] *Id.* at 63.
[13] *See* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] The White House, *Executive Order – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017), *available at* https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal (last visited June 29, 2017).

security of federal systems may nevertheless be undermined by compromised anti-virus products. Government contracting data indicating that several federal departments and agencies use or have used cybersecurity or anti-virus products manufactured by Kaspersky Lab is even more troubling.[18] If federal agencies and departments are being guarded by potentially compromised software, then it is virtually impossible for such agencies to effectively and efficiently implement the NIST Framework, and to fully comply with President Trump's executive order. The recent news that Kaspersky Lab's products have been removed from the General Service Administration's contracting Schedule 67 and 70 is encouraging, however federal agencies and contractors may be likely to continue use of Kaspersky Lab's products.[19]

Cybersecurity is a greater threat to our nation than ever before. If these widely reported allegations prove true, then the American public has ample grounds on which to rest their concerns about the security of data stored and transmitted on federal information systems—especially those allegedly protected by Kaspersky Lab's products. In light of this increasing threat, the Committee takes seriously its duty to ensure the NIST Cybersecurity Framework is properly equipped and adapted to safeguard our nation's information. To assist the Committee in understanding the effectiveness of the NIST Framework, and potential vulnerabilities that exist on federal information systems, please provide the following documents and information as soon as possible, but no later than August 11, 2017. Please provide the requested materials for the time frame from January 1, 2013, to present:

1. All documents and communications referring or relating to cybersecurity and/or anti-virus products manufactured by Kaspersky Lab.

2. All documents and communications referring or relating to any evaluation, risk assessment, and decision-making processes on the matter of whether to implement products manufactured by Kaspersky Lab.

3. All documents and communications referring or relating to the use or implementation of products manufactured by Kaspersky Lab.

---

[18] Government Contracting Dataset, *available at* https://www.usaspending.gov/Pages/AdvancedSearch.aspx?k=kaspersky (last visited June 29, 2017); *see* David Goldstein & Greg Gordon, *Exclusive: Kremlin Documents Suggest Link Between Cyber Giant and Russia Spy Agency*, MCCLATCHY, July 3, 2017, *available at* http://www.mcclatchydc.com/news/nation-world/national/article159342694.html (last visited July 12, 2017); *see also* Mike Levine & Pierre Thomas, *Officials Fear Russia Could Try To Target US Through Popular Software Firm Under FBI Scrutiny*, ABC NEWS, May 9, 2017, *available at* http://abcnews.go.com/US/officials-fear-russia-target-us-popular-software-firm/story?id=47295729 (last visited July 12, 2017).

[19] *See* Sarah Kuranda, *Kaspersky Lab Removed From GSA Schedule, Limiting Federal Sales for Its Security Software*, CRN, July 12, 2017, *available at* http://www.crn.com/news/security/300088591/kaspersky-removed-from-gsa-schedule-limiting-federal-sales-for-its-security-software.htm; *see also* Eric Geller, *Trump Administration Restricts Popular Russian Security Software*, POLITICO, July 11, 2017, *available at* http://www.politico.com/story/2017/07/11/trump-russian-security-software-240423.

4. A complete list of any computers, systems, data, media, and/or information utilizing or accessible to Kaspersky Lab products or services.

5. Identify any federal government contractors or subcontractors known to be utilizing Kaspersky Lab's products to fulfill requirements of contracts with the Department or Agency.

6. All documents and communications referring or relating to the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity.

7. All documents and communications referring or relating to the production of reports required by Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.

Pursuant to House Rule X, the Committee on Science, Space, and Technology has jurisdiction over National Institute of Standards and Technology which develops cybersecurity standards and guidelines for the federal government and recommendations for the private sector.

When producing documents to the Committee, please deliver production sets to the Majority Staff in Room 2321 of the Rayburn House Office Building and the Minority Staff in Room 394 of the Ford House Office Building. The Committee prefers, if possible, to receive all documents in electronic format.

If you have any questions about this request, please contact Drew Colliatie or Tom Connally at 202-225-6371. Thank you for your attention to this matter.

Sincerely,

Lamar Smith

Lamar Smith
Chairman

cc: The Honorable Eddie Bernice Johnson, Ranking Minority Member

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6301
(202) 225–6371
www.science.house.gov

July 27, 2017

The Honorable Rick Perry
Secretary
U.S. Department of Energy
1000 Independence Avenue SW
Washington D.C. 20585

Dear Secretary Perry,

As part of an ongoing review of the federal government's cybersecurity policies and standards, the Committee on Science, Space, and Technology is requesting information and documents from the Department regarding Kaspersky Lab. The Committee is charged with oversight of the National Institute of Standards and Technology (NIST), and continuously evaluates whether changes to the Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework) are necessary. The documents and information will assist the Committee in determining whether the Framework requires further refinement when implemented by federal departments and agencies.

Kaspersky Lab is among the world's largest cybersecurity companies. Headquartered in Moscow, Russia, it services approximately 400 million users worldwide, including a number of United States Government Agencies and entities.[1] Kaspersky Lab specializes in anti-virus software—products with potentially uninhibited access to the systems they protect.[2] Although Kaspersky Lab was once considered a reputable cybersecurity firm, several concerns have been raised regarding the company and Eugene Kaspersky—the founder and CEO of Kaspersky Lab—and his potential ties to the Russian government.

The Committee is concerned that Kaspersky Lab is susceptible to manipulation by the Russian government, and that its products could be used as a tool for espionage, sabotage, or other nefarious activities against the United States. As early as 2015, reports began to surface

---

[1] *See* Jordan Robertson, *A Russian Cybersecurity Company's Ties to the Kremlin*, BLOOMBERG GOVERNMENT, Jul. 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSXAKB6JIJVL (last visited July 11, 2017).
[2] *See* Jordan Robertson & Michael Riley, *Kaspersky Lab Has Been Working With Russian Intelligence*, BLOOMBERG GOVERNMENT, July 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSX50G6KLVR5 (last visited July 11, 2017).

alleging that Mr. Kaspersky may have "close ties to Russian spies."[3] Shortly thereafter, *Reuters* reported that Kaspersky Lab engaged in a "sabotage" campaign undoubtedly targeting the U.S. cybersecurity market.[4] Specifically, the company "tried to damage rivals in the marketplace by tricking their antivirus software programs into classifying benign files as malicious."[5] More recently, Russia's alleged interference in the 2016 presidential election has heightened public concerns about the Kremlin's desire to meddle with American democratic processes. This, in turn, has ignited speculation over America's cybersecurity posture, and the potential ties that Kaspersky Lab has with the Kremlin. Namely, that the Russian government could use products manufactured by Kaspersky Lab as a medium for engaging in nefarious cyber campaigns against U.S. information systems—including those at several federal departments and agencies—that are purportedly protected by the company's products.[6] Adding to concern, the FBI sent agents to visit "at least a dozen employees of Kaspersky" in order to question them "about the company's operations as part of a counter-intelligence inquiry."[7]

Given the increasing prevalence of cybersecurity threats across the nation, the federal government's use of cybersecurity products manufactured by a firm with potential ties to the Russian government is concerning to Congress. In May, the Senate Intelligence Committee held an open hearing where several top U.S. intelligence officials stated with consensus that they would not be comfortable using Kaspersky Lab's products on their systems.[8] Additionally, on June 15, 2017, the House Science Committee Subcommittees on Oversight and Research and Technology held a joint hearing where cybersecurity experts testified on industry approaches and

---

[3] Carol Matlack, *The Company Securing Your Internet Has Close Ties to Russian Spies*, BLOOMBERG BUSINESSWEEK, Mar. 19, 2015, *available at* https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies (last visited June 19, 2017).

[4] Joseph Menn, *Exclusive: Russian Antivirus Firm Faked Malware to Harm Rivals*, REUTERS, Aug. 14, 2015, *available at* www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QJ1CR20150814 (last visited June 27, 2017); *see also* Joseph Menn, *Exclusive: Russia's Kaspersky Threatened to 'Rub Out' Rival, Email Shows*, REUTERS, Aug. 28, 2015, *available at* http://www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QX2GO20150828 (last visited June 27, 2017).

[5] *Id.*

[6] *See* Ali Watkins, *US Officials Are Warning About A Russian Cybersecurity Company's US Government Ties*, BUZZFEED NEWS, May 8, 2017, *available at* https://www.buzzfeed.com/alimwatkins/us-officials-are-warning-about-a-russian-cybersecurity?utm_term=.osyYrP2Mz6#.kexPnOw1Lk (last visited June 19, 2017); *see also* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).

[7] Ken Dilanian & Tom Winter, *Bill Would Bar Pentagon From Business With Russian Cyber Firm Kaspersky*, NBC NEWS, June 28, 2017, *available at* http://www.nbcnews.com/news/us-news/fbi-interviews-employees-russia-linked-cyber-security-firm-kaspersky-lab-n777571 (last visited June 29, 2017); *see also* Joe Uchill, *FBI Visits Kaspersky Lab Employees*, THE HILL, June 28, 2017, *available at* http://thehill.com/policy/cybersecurity/339887-fbi-visits-kaspersky-lab-employees (last visited June 29, 2017).

[8] S. Comm. on Intel., *Worldwide Threats Hearing*, 115th Cong. (May 11, 2017). (question and answer by Senator Marco Rubio).

best practices for safeguarding against future cyber threats.[9] Among the panel of expert witnesses was Salim Neino, CEO of Kryptos Logic—the cybersecurity firm whose employee helped thwart further propagation of the recent WannaCry ransomware attack.[10] In response to questions about the ability of a software manufacturer to embed a "backdoor" into anti-virus software—to facilitate a State's cyber-espionage activities—Mr. Neino alarmingly affirmed that he had "seen that a multitude of times" in the past, and that the barriers to engaging in such activities are "very low."[11] This revelation gives the Committee great concern, especially in light of the capabilities that anti-virus software possesses. Additionally, in response to a question regarding Kaspersky Lab, retired Army General Gregory Touhill, the first federal chief information security officer or CISO, told the Committee: "I buy American."[12]

Anti-virus software is extremely powerful and operates by scanning files at the system level, rather than on the network periphery.[13] As such, other security systems generally do not monitor the operations carried out by the anti-virus software.[14] From a practical perspective, this means that compromised anti-virus software could be used for malicious or nefarious purposes, and could do so without detection. If anti-virus technology or systems are compromised by a user's adversary, it could install malicious code disguised as a security update; it could forego specific updates to pave the way for use of certain vectors of attack; it could forego beneficial updates for a specified subset of users; and it could even extract data that a user's adversary considers valuable.[15] Furthermore, anti-virus is so powerful that it has nearly unimpeded access into all attachments, files, and information contained on a system.[16] In sum, compromised anti-virus has the potential to undermine the security and integrity of any system on which it is installed.

The security and integrity of federal information systems are only as strong as the products that guard them. Although Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, requires federal departments and agencies to implement the NIST Cybersecurity Framework and to provide reports related thereto,[17] the

---

[9] H. Comm. on Science, Space, & Tech. Subcomm. on Research & Tech. jointly with the Subcomm. on Oversight, *Hearing on Bolstering the Government's Cybersecurity: Lessons Learned from WannaCry*, Preliminary Hearing Transcript, 115th Cong. (June 15, 2017) at 61.
[10] *Id.*
[11] *Id.* at 62 (question and answer by Representative Clay Higgins).
[12] *Id.* at 63.
[13] *See* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] The White House, *Executive Order – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017), *available at* https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal (last visited June 29, 2017).

security of federal systems may nevertheless be undermined by compromised anti-virus products. Government contracting data indicating that several federal departments and agencies use or have used cybersecurity or anti-virus products manufactured by Kaspersky Lab is even more troubling.[18] If federal agencies and departments are being guarded by potentially compromised software, then it is virtually impossible for such agencies to effectively and efficiently implement the NIST Framework, and to fully comply with President Trump's executive order. The recent news that Kaspersky Lab's products have been removed from the General Service Administration's contracting Schedule 67 and 70 is encouraging, however federal agencies and contractors may be likely to continue use of Kaspersky Lab's products.[19]

Cybersecurity is a greater threat to our nation than ever before. If these widely reported allegations prove true, then the American public has ample grounds on which to rest their concerns about the security of data stored and transmitted on federal information systems—especially those allegedly protected by Kaspersky Lab's products. In light of this increasing threat, the Committee takes seriously its duty to ensure the NIST Cybersecurity Framework is properly equipped and adapted to safeguard our nation's information. To assist the Committee in understanding the effectiveness of the NIST Framework, and potential vulnerabilities that exist on federal information systems, please provide the following documents and information as soon as possible, but no later than August 11, 2017. Please provide the requested materials for the time frame from January 1, 2013, to present:

1. All documents and communications referring or relating to cybersecurity and/or anti-virus products manufactured by Kaspersky Lab.

2. All documents and communications referring or relating to any evaluation, risk assessment, and decision-making processes on the matter of whether to implement products manufactured by Kaspersky Lab.

3. All documents and communications referring or relating to the use or implementation of products manufactured by Kaspersky Lab.

---

[18] Government Contracting Dataset, *available at* https://www.usaspending.gov/Pages/AdvancedSearch.aspx?k=kaspersky (last visited June 29, 2017); *see* David Goldstein & Greg Gordon, *Exclusive: Kremlin Documents Suggest Link Between Cyber Giant and Russia Spy Agency*, MCCLATCHY, July 3, 2017, *available at* http://www.mcclatchydc.com/news/nation-world/national/article159342694.html (last visited July 12, 2017); *see also* Mike Levine & Pierre Thomas, *Officials Fear Russia Could Try To Target US Through Popular Software Firm Under FBI Scrutiny*, ABC NEWS, May 9, 2017, *available at* http://abcnews.go.com/US/officials-fear-russia-target-us-popular-software-firm/story?id=47295729 (last visited July 12, 2017).

[19] *See* Sarah Kuranda, *Kaspersky Lab Removed From GSA Schedule, Limiting Federal Sales for Its Security Software*, CRN, July 12, 2017, *available at* http://www.crn.com/news/security/300088591/kaspersky-removed-from-gsa-schedule-limiting-federal-sales-for-its-security-software.htm; *see also* Eric Geller, *Trump Administration Restricts Popular Russian Security Software*, POLITICO, July 11, 2017, *available at* http://www.politico.com/story/2017/07/11/trump-russian-security-software-240423.

4. A complete list of any computers, systems, data, media, and/or information utilizing or accessible to Kaspersky Lab products or services.

5. Identify any federal government contractors or subcontractors known to be utilizing Kaspersky Lab's products to fulfill requirements of contracts with the Department or Agency.

6. All documents and communications referring or relating to the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity.

7. All documents and communications referring or relating to the production of reports required by Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.

Pursuant to House Rule X, the Committee on Science, Space, and Technology has jurisdiction over National Institute of Standards and Technology which develops cybersecurity standards and guidelines for the federal government and recommendations for the private sector.

When producing documents to the Committee, please deliver production sets to the Majority Staff in Room 2321 of the Rayburn House Office Building and the Minority Staff in Room 394 of the Ford House Office Building. The Committee prefers, if possible, to receive all documents in electronic format.

If you have any questions about this request, please contact Drew Colliatie or Tom Connally at 202-225-6371. Thank you for your attention to this matter.

Sincerely,

Lamar Smith

Lamar Smith
Chairman

cc: The Honorable Eddie Bernice Johnson, Ranking Minority Member

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6301
(202) 225–6371
www.science.house.gov

July 27, 2017

The Honorable Jefferson Beauregard Sessions, III
Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington D.C. 20530 - 0001

Dear Attorney General Sessions,

As part of an ongoing review of the federal government's cybersecurity policies and standards, the Committee on Science, Space, and Technology is requesting information and documents from the Department regarding Kaspersky Lab. The Committee is charged with oversight of the National Institute of Standards and Technology (NIST), and continuously evaluates whether changes to the Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework) are necessary. The documents and information will assist the Committee in determining whether the Framework requires further refinement when implemented by federal departments and agencies.

Kaspersky Lab is among the world's largest cybersecurity companies. Headquartered in Moscow, Russia, it services approximately 400 million users worldwide, including a number of United States Government Agencies and entities.[1] Kaspersky Lab specializes in anti-virus software—products with potentially uninhibited access to the systems they protect.[2] Although Kaspersky Lab was once considered a reputable cybersecurity firm, several concerns have been raised regarding the company and Eugene Kaspersky—the founder and CEO of Kaspersky Lab—and his potential ties to the Russian government.

The Committee is concerned that Kaspersky Lab is susceptible to manipulation by the Russian government, and that its products could be used as a tool for espionage, sabotage, or other nefarious activities against the United States. As early as 2015, reports began to surface

---

[1] *See* Jordan Robertson, *A Russian Cybersecurity Company's Ties to the Kremlin*, BLOOMBERG GOVERNMENT, Jul. 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSXAKB6JIJVL (last visited July 11, 2017).
[2] *See* Jordan Robertson & Michael Riley, *Kaspersky Lab Has Been Working With Russian Intelligence*, BLOOMBERG GOVERNMENT, July 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSX50G6KLVR5 (last visited July 11, 2017).

alleging that Mr. Kaspersky may have "close ties to Russian spies."[3] Shortly thereafter, *Reuters* reported that Kaspersky Lab engaged in a "sabotage" campaign undoubtedly targeting the U.S. cybersecurity market.[4] Specifically, the company "tried to damage rivals in the marketplace by tricking their antivirus software programs into classifying benign files as malicious."[5] More recently, Russia's alleged interference in the 2016 presidential election has heightened public concerns about the Kremlin's desire to meddle with American democratic processes. This, in turn, has ignited speculation over America's cybersecurity posture, and the potential ties that Kaspersky Lab has with the Kremlin. Namely, that the Russian government could use products manufactured by Kaspersky Lab as a medium for engaging in nefarious cyber campaigns against U.S. information systems—including those at several federal departments and agencies—that are purportedly protected by the company's products.[6] Adding to concern, the FBI sent agents to visit "at least a dozen employees of Kaspersky" in order to question them "about the company's operations as part of a counter-intelligence inquiry."[7]

Given the increasing prevalence of cybersecurity threats across the nation, the federal government's use of cybersecurity products manufactured by a firm with potential ties to the Russian government is concerning to Congress. In May, the Senate Intelligence Committee held an open hearing where several top U.S. intelligence officials stated with consensus that they would not be comfortable using Kaspersky Lab's products on their systems.[8] Additionally, on June 15, 2017, the House Science Committee Subcommittees on Oversight and Research and Technology held a joint hearing where cybersecurity experts testified on industry approaches and

---

[3] Carol Matlack, *The Company Securing Your Internet Has Close Ties to Russian Spies*, BLOOMBERG BUSINESSWEEK, Mar. 19, 2015, *available at* https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies (last visited June 19, 2017).

[4] Joseph Menn, *Exclusive: Russian Antivirus Firm Faked Malware to Harm Rivals*, REUTERS, Aug. 14, 2015, *available at* www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QJ1CR20150814 (last visited June 27, 2017); *see also* Joseph Menn, *Exclusive: Russia's Kaspersky Threatened to 'Rub Out' Rival, Email Shows*, REUTERS, Aug. 28, 2015, *available at* http://www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QX2GO20150828 (last visited June 27, 2017).

[5] *Id.*

[6] *See* Ali Watkins, *US Officials Are Warning About A Russian Cybersecurity Company's US Government Ties*, BUZZFEED NEWS, May 8, 2017, *available at* https://www.buzzfeed.com/alimwatkins/us-officials-are-warning-about-a-russian-cybersecurity?utm_term=.osyYrP2Mz6#.kexPnOw1Lk (last visited June 19, 2017); *see also* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).

[7] Ken Dilanian & Tom Winter, *Bill Would Bar Pentagon From Business With Russian Cyber Firm Kaspersky*, NBC NEWS, June 28, 2017, *available at* http://www.nbcnews.com/news/us-news/fbi-interviews-employees-russia-linked-cyber-security-firm-kaspersky-lab-n777571 (last visited June 29, 2017); *see also* Joe Uchill, *FBI Visits Kaspersky Lab Employees*, THE HILL, June 28, 2017, *available at* http://thehill.com/policy/cybersecurity/339887-fbi-visits-kaspersky-lab-employees (last visited June 29, 2017).

[8] S. Comm. on Intel., *Worldwide Threats Hearing*, 115th Cong. (May 11, 2017). (question and answer by Senator Marco Rubio).

best practices for safeguarding against future cyber threats.[9] Among the panel of expert witnesses was Salim Neino, CEO of Kryptos Logic—the cybersecurity firm whose employee helped thwart further propagation of the recent WannaCry ransomware attack.[10] In response to questions about the ability of a software manufacturer to embed a "backdoor" into anti-virus software—to facilitate a State's cyber-espionage activities—Mr. Neino alarmingly affirmed that he had "seen that a multitude of times" in the past, and that the barriers to engaging in such activities are "very low."[11] This revelation gives the Committee great concern, especially in light of the capabilities that anti-virus software possesses. Additionally, in response to a question regarding Kaspersky Lab, retired Army General Gregory Touhill, the first federal chief information security officer or CISO, told the Committee: "I buy American."[12]

Anti-virus software is extremely powerful and operates by scanning files at the system level, rather than on the network periphery.[13] As such, other security systems generally do not monitor the operations carried out by the anti-virus software.[14] From a practical perspective, this means that compromised anti-virus software could be used for malicious or nefarious purposes, and could do so without detection. If anti-virus technology or systems are compromised by a user's adversary, it could install malicious code disguised as a security update; it could forego specific updates to pave the way for use of certain vectors of attack; it could forego beneficial updates for a specified subset of users; and it could even extract data that a user's adversary considers valuable.[15] Furthermore, anti-virus is so powerful that it has nearly unimpeded access into all attachments, files, and information contained on a system.[16] In sum, compromised anti-virus has the potential to undermine the security and integrity of any system on which it is installed.

The security and integrity of federal information systems are only as strong as the products that guard them. Although Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, requires federal departments and agencies to implement the NIST Cybersecurity Framework and to provide reports related thereto,[17] the

---

[9] H. Comm. on Science, Space, & Tech. Subcomm. on Research & Tech. jointly with the Subcomm. on Oversight, *Hearing on Bolstering the Government's Cybersecurity: Lessons Learned from WannaCry*, Preliminary Hearing Transcript, 115th Cong. (June 15, 2017) at 61.
[10] *Id.*
[11] *Id.* at 62 (question and answer by Representative Clay Higgins).
[12] *Id.* at 63.
[13] *See* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] The White House, *Executive Order – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017), *available at* https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal (last visited June 29, 2017).

security of federal systems may nevertheless be undermined by compromised anti-virus products. Government contracting data indicating that several federal departments and agencies use or have used cybersecurity or anti-virus products manufactured by Kaspersky Lab is even more troubling.[18] If federal agencies and departments are being guarded by potentially compromised software, then it is virtually impossible for such agencies to effectively and efficiently implement the NIST Framework, and to fully comply with President Trump's executive order. The recent news that Kaspersky Lab's products have been removed from the General Service Administration's contracting Schedule 67 and 70 is encouraging, however federal agencies and contractors may be likely to continue use of Kaspersky Lab's products.[19]

Cybersecurity is a greater threat to our nation than ever before. If these widely reported allegations prove true, then the American public has ample grounds on which to rest their concerns about the security of data stored and transmitted on federal information systems—especially those allegedly protected by Kaspersky Lab's products. In light of this increasing threat, the Committee takes seriously its duty to ensure the NIST Cybersecurity Framework is properly equipped and adapted to safeguard our nation's information. To assist the Committee in understanding the effectiveness of the NIST Framework, and potential vulnerabilities that exist on federal information systems, please provide the following documents and information as soon as possible, but no later than August 11, 2017. Please provide the requested materials for the time frame from January 1, 2013, to present:

1. All documents and communications referring or relating to cybersecurity and/or anti-virus products manufactured by Kaspersky Lab.

2. All documents and communications referring or relating to any evaluation, risk assessment, and decision-making processes on the matter of whether to implement products manufactured by Kaspersky Lab.

3. All documents and communications referring or relating to the use or implementation of products manufactured by Kaspersky Lab.

---

[18] Government Contracting Dataset, *available at* https://www.usaspending.gov/Pages/AdvancedSearch.aspx?k=kaspersky (last visited June 29, 2017); *see* David Goldstein & Greg Gordon, *Exclusive: Kremlin Documents Suggest Link Between Cyber Giant and Russia Spy Agency*, MCCLATCHY, July 3, 2017, *available at* http://www.mcclatchydc.com/news/nation-world/national/article159342694.html (last visited July 12, 2017); *see also* Mike Levine & Pierre Thomas, *Officials Fear Russia Could Try To Target US Through Popular Software Firm Under FBI Scrutiny*, ABC NEWS, May 9, 2017, *available at* http://abcnews.go.com/US/officials-fear-russia-target-us-popular-software-firm/story?id=47295729 (last visited July 12, 2017).

[19] *See* Sarah Kuranda, *Kaspersky Lab Removed From GSA Schedule, Limiting Federal Sales for Its Security Software*, CRN, July 12, 2017, *available at* http://www.crn.com/news/security/300088591/kaspersky-removed-from-gsa-schedule-limiting-federal-sales-for-its-security-software.htm; *see also* Eric Geller, *Trump Administration Restricts Popular Russian Security Software*, POLITICO, July 11, 2017, *available at* http://www.politico.com/story/2017/07/11/trump-russian-security-software-240423.

4. A complete list of any computers, systems, data, media, and/or information utilizing or accessible to Kaspersky Lab products or services.

5. Identify any federal government contractors or subcontractors known to be utilizing Kaspersky Lab's products to fulfill requirements of contracts with the Department or Agency.

6. All documents and communications referring or relating to the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity.

7. All documents and communications referring or relating to the production of reports required by Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.

Pursuant to House Rule X, the Committee on Science, Space, and Technology has jurisdiction over National Institute of Standards and Technology which develops cybersecurity standards and guidelines for the federal government and recommendations for the private sector.

When producing documents to the Committee, please deliver production sets to the Majority Staff in Room 2321 of the Rayburn House Office Building and the Minority Staff in Room 394 of the Ford House Office Building. The Committee prefers, if possible, to receive all documents in electronic format.

If you have any questions about this request, please contact Drew Colliatie or Tom Connally at 202-225-6371. Thank you for your attention to this matter.

Sincerely,

Lamar Smith
Chairman

cc: The Honorable Eddie Bernice Johnson, Ranking Minority Member

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6301
(202) 225–6371
www.science.house.gov

July 27, 2017

The Honorable R. Alexander Acosta
Secretary
U.S. Department of Labor
200 Constitution Ave NW
Washington D.C. 20210

Dear Secretary Acosta,

As part of an ongoing review of the federal government's cybersecurity policies and standards, the Committee on Science, Space, and Technology is requesting information and documents from the Department regarding Kaspersky Lab. The Committee is charged with oversight of the National Institute of Standards and Technology (NIST), and continuously evaluates whether changes to the Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework) are necessary. The documents and information will assist the Committee in determining whether the Framework requires further refinement when implemented by federal departments and agencies.

Kaspersky Lab is among the world's largest cybersecurity companies. Headquartered in Moscow, Russia, it services approximately 400 million users worldwide, including a number of United States Government Agencies and entities.[1] Kaspersky Lab specializes in anti-virus software—products with potentially uninhibited access to the systems they protect.[2] Although Kaspersky Lab was once considered a reputable cybersecurity firm, several concerns have been raised regarding the company and Eugene Kaspersky—the founder and CEO of Kaspersky Lab—and his potential ties to the Russian government.

The Committee is concerned that Kaspersky Lab is susceptible to manipulation by the Russian government, and that its products could be used as a tool for espionage, sabotage, or other nefarious activities against the United States. As early as 2015, reports began to surface

---

[1] *See* Jordan Robertson, *A Russian Cybersecurity Company's Ties to the Kremlin*, BLOOMBERG GOVERNMENT, Jul. 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSXAKB6JIJVL (last visited July 11, 2017).
[2] *See* Jordan Robertson & Michael Riley, *Kaspersky Lab Has Been Working With Russian Intelligence*, BLOOMBERG GOVERNMENT, July 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSX50G6KLVR5 (last visited July 11, 2017).

alleging that Mr. Kaspersky may have "close ties to Russian spies."[3] Shortly thereafter, *Reuters* reported that Kaspersky Lab engaged in a "sabotage" campaign undoubtedly targeting the U.S. cybersecurity market.[4] Specifically, the company "tried to damage rivals in the marketplace by tricking their antivirus software programs into classifying benign files as malicious."[5] More recently, Russia's alleged interference in the 2016 presidential election has heightened public concerns about the Kremlin's desire to meddle with American democratic processes. This, in turn, has ignited speculation over America's cybersecurity posture, and the potential ties that Kaspersky Lab has with the Kremlin. Namely, that the Russian government could use products manufactured by Kaspersky Lab as a medium for engaging in nefarious cyber campaigns against U.S. information systems—including those at several federal departments and agencies—that are purportedly protected by the company's products.[6] Adding to concern, the FBI sent agents to visit "at least a dozen employees of Kaspersky" in order to question them "about the company's operations as part of a counter-intelligence inquiry."[7]

Given the increasing prevalence of cybersecurity threats across the nation, the federal government's use of cybersecurity products manufactured by a firm with potential ties to the Russian government is concerning to Congress. In May, the Senate Intelligence Committee held an open hearing where several top U.S. intelligence officials stated with consensus that they would not be comfortable using Kaspersky Lab's products on their systems.[8] Additionally, on June 15, 2017, the House Science Committee Subcommittees on Oversight and Research and Technology held a joint hearing where cybersecurity experts testified on industry approaches and

---

[3] Carol Matlack, *The Company Securing Your Internet Has Close Ties to Russian Spies*, BLOOMBERG BUSINESSWEEK, Mar. 19, 2015, *available at* https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies (last visited June 19, 2017).

[4] Joseph Menn, *Exclusive: Russian Antivirus Firm Faked Malware to Harm Rivals*, REUTERS, Aug. 14, 2015, *available at* www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QJ1CR20150814 (last visited June 27, 2017); *see also* Joseph Menn, *Exclusive: Russia's Kaspersky Threatened to 'Rub Out' Rival, Email Shows*, REUTERS, Aug. 28, 2015, *available at* http://www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QX2GO20150828 (last visited June 27, 2017).

[5] *Id.*

[6] *See* Ali Watkins, *US Officials Are Warning About A Russian Cybersecurity Company's US Government Ties*, BUZZFEED NEWS, May 8, 2017, *available at* https://www.buzzfeed.com/alimwatkins/us-officials-are-warning-about-a-russian-cybersecurity?utm_term=.osyYrP2Mz6#.kexPnOw1Lk (last visited June 19, 2017); *see also* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).

[7] Ken Dilanian & Tom Winter, *Bill Would Bar Pentagon From Business With Russian Cyber Firm Kaspersky*, NBC NEWS, June 28, 2017, *available at* http://www.nbcnews.com/news/us-news/fbi-interviews-employees-russia-linked-cyber-security-firm-kaspersky-lab-n777571 (last visited June 29, 2017); *see also* Joe Uchill, *FBI Visits Kaspersky Lab Employees*, THE HILL, June 28, 2017, *available at* http://thehill.com/policy/cybersecurity/339887-fbi-visits-kaspersky-lab-employees (last visited June 29, 2017).

[8] S. Comm. on Intel., *Worldwide Threats Hearing*, 115th Cong. (May 11, 2017). (question and answer by Senator Marco Rubio).

best practices for safeguarding against future cyber threats.[9] Among the panel of expert witnesses was Salim Neino, CEO of Kryptos Logic—the cybersecurity firm whose employee helped thwart further propagation of the recent WannaCry ransomware attack.[10] In response to questions about the ability of a software manufacturer to embed a "backdoor" into anti-virus software—to facilitate a State's cyber-espionage activities—Mr. Neino alarmingly affirmed that he had "seen that a multitude of times" in the past, and that the barriers to engaging in such activities are "very low."[11] This revelation gives the Committee great concern, especially in light of the capabilities that anti-virus software possesses. Additionally, in response to a question regarding Kaspersky Lab, retired Army General Gregory Touhill, the first federal chief information security officer or CISO, told the Committee: "I buy American."[12]

Anti-virus software is extremely powerful and operates by scanning files at the system level, rather than on the network periphery.[13] As such, other security systems generally do not monitor the operations carried out by the anti-virus software.[14] From a practical perspective, this means that compromised anti-virus software could be used for malicious or nefarious purposes, and could do so without detection. If anti-virus technology or systems are compromised by a user's adversary, it could install malicious code disguised as a security update; it could forego specific updates to pave the way for use of certain vectors of attack; it could forego beneficial updates for a specified subset of users; and it could even extract data that a user's adversary considers valuable.[15] Furthermore, anti-virus is so powerful that it has nearly unimpeded access into all attachments, files, and information contained on a system.[16] In sum, compromised anti-virus has the potential to undermine the security and integrity of any system on which it is installed.

The security and integrity of federal information systems are only as strong as the products that guard them. Although Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, requires federal departments and agencies to implement the NIST Cybersecurity Framework and to provide reports related thereto,[17] the

---

[9] H. Comm. on Science, Space, & Tech. Subcomm. on Research & Tech. jointly with the Subcomm. on Oversight, *Hearing on Bolstering the Government's Cybersecurity: Lessons Learned from WannaCry*, Preliminary Hearing Transcript, 115th Cong. (June 15, 2017) at 61.

[10] *Id.*

[11] *Id.* at 62 (question and answer by Representative Clay Higgins).

[12] *Id.* at 63.

[13] *See* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).

[14] *Id.*

[15] *Id.*

[16] *Id.*

[17] The White House, *Executive Order – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017), *available at* https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal (last visited June 29, 2017).

security of federal systems may nevertheless be undermined by compromised anti-virus products. Government contracting data indicating that several federal departments and agencies use or have used cybersecurity or anti-virus products manufactured by Kaspersky Lab is even more troubling.[18] If federal agencies and departments are being guarded by potentially compromised software, then it is virtually impossible for such agencies to effectively and efficiently implement the NIST Framework, and to fully comply with President Trump's executive order. The recent news that Kaspersky Lab's products have been removed from the General Service Administration's contracting Schedule 67 and 70 is encouraging, however federal agencies and contractors may be likely to continue use of Kaspersky Lab's products.[19]

Cybersecurity is a greater threat to our nation than ever before. If these widely reported allegations prove true, then the American public has ample grounds on which to rest their concerns about the security of data stored and transmitted on federal information systems—especially those allegedly protected by Kaspersky Lab's products. In light of this increasing threat, the Committee takes seriously its duty to ensure the NIST Cybersecurity Framework is properly equipped and adapted to safeguard our nation's information. To assist the Committee in understanding the effectiveness of the NIST Framework, and potential vulnerabilities that exist on federal information systems, please provide the following documents and information as soon as possible, but no later than August 11, 2017. Please provide the requested materials for the time frame from January 1, 2013, to present:

1. All documents and communications referring or relating to cybersecurity and/or anti-virus products manufactured by Kaspersky Lab.

2. All documents and communications referring or relating to any evaluation, risk assessment, and decision-making processes on the matter of whether to implement products manufactured by Kaspersky Lab.

3. All documents and communications referring or relating to the use or implementation of products manufactured by Kaspersky Lab.

---

[18] Government Contracting Dataset, *available at* https://www.usaspending.gov/Pages/AdvancedSearch.aspx?k=kaspersky (last visited June 29, 2017); *see* David Goldstein & Greg Gordon, *Exclusive: Kremlin Documents Suggest Link Between Cyber Giant and Russia Spy Agency*, MCCLATCHY, July 3, 2017, *available at* http://www.mcclatchydc.com/news/nation-world/national/article159342694.html (last visited July 12, 2017); *see also* Mike Levine & Pierre Thomas, *Officials Fear Russia Could Try To Target US Through Popular Software Firm Under FBI Scrutiny*, ABC NEWS, May 9, 2017, *available at* http://abcnews.go.com/US/officials-fear-russia-target-us-popular-software-firm/story?id=47295729 (last visited July 12, 2017).

[19] *See* Sarah Kuranda, *Kaspersky Lab Removed From GSA Schedule, Limiting Federal Sales for Its Security Software*, CRN, July 12, 2017, *available at* http://www.crn.com/news/security/300088591/kaspersky-removed-from-gsa-schedule-limiting-federal-sales-for-its-security-software.htm; *see also* Eric Geller, *Trump Administration Restricts Popular Russian Security Software*, POLITICO, July 11, 2017, *available at* http://www.politico.com/story/2017/07/11/trump-russian-security-software-240423.

4. A complete list of any computers, systems, data, media, and/or information utilizing or accessible to Kaspersky Lab products or services.

5. Identify any federal government contractors or subcontractors known to be utilizing Kaspersky Lab's products to fulfill requirements of contracts with the Department or Agency.

6. All documents and communications referring or relating to the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity.

7. All documents and communications referring or relating to the production of reports required by Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.

Pursuant to House Rule X, the Committee on Science, Space, and Technology has jurisdiction over National Institute of Standards and Technology which develops cybersecurity standards and guidelines for the federal government and recommendations for the private sector.

When producing documents to the Committee, please deliver production sets to the Majority Staff in Room 2321 of the Rayburn House Office Building and the Minority Staff in Room 394 of the Ford House Office Building. The Committee prefers, if possible, to receive all documents in electronic format.

If you have any questions about this request, please contact Drew Colliatie or Tom Connally at 202-225-6371. Thank you for your attention to this matter.

Sincerely,

Lamar Smith

Lamar Smith
Chairman

cc: The Honorable Eddie Bernice Johnson, Ranking Minority Member

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6301
(202) 225-6371
www.science.house.gov

July 27, 2017

The Honorable Elaine L. Chao
Secretary
U.S. Department of Transportation
1200 New Jersey Avenue SE
Washington D.C. 20590

Dear Secretary Chao,

As part of an ongoing review of the federal government's cybersecurity policies and standards, the Committee on Science, Space, and Technology is requesting information and documents from the Department regarding Kaspersky Lab. The Committee is charged with oversight of the National Institute of Standards and Technology (NIST), and continuously evaluates whether changes to the Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework) are necessary. The documents and information will assist the Committee in determining whether the Framework requires further refinement when implemented by federal departments and agencies.

Kaspersky Lab is among the world's largest cybersecurity companies. Headquartered in Moscow, Russia, it services approximately 400 million users worldwide, including a number of United States Government Agencies and entities.[1] Kaspersky Lab specializes in anti-virus software—products with potentially uninhibited access to the systems they protect.[2] Although Kaspersky Lab was once considered a reputable cybersecurity firm, several concerns have been raised regarding the company and Eugene Kaspersky—the founder and CEO of Kaspersky Lab—and his potential ties to the Russian government.

The Committee is concerned that Kaspersky Lab is susceptible to manipulation by the Russian government, and that its products could be used as a tool for espionage, sabotage, or other nefarious activities against the United States. As early as 2015, reports began to surface

---

[1] *See* Jordan Robertson, *A Russian Cybersecurity Company's Ties to the Kremlin*, BLOOMBERG GOVERNMENT, Jul. 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSXAKB6JIJVL (last visited July 11, 2017).
[2] *See* Jordan Robertson & Michael Riley, *Kaspersky Lab Has Been Working With Russian Intelligence*, BLOOMBERG GOVERNMENT, July 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSX50G6KLVR5 (last visited July 11, 2017).

alleging that Mr. Kaspersky may have "close ties to Russian spies."[3] Shortly thereafter, *Reuters* reported that Kaspersky Lab engaged in a "sabotage" campaign undoubtedly targeting the U.S. cybersecurity market.[4] Specifically, the company "tried to damage rivals in the marketplace by tricking their antivirus software programs into classifying benign files as malicious."[5] More recently, Russia's alleged interference in the 2016 presidential election has heightened public concerns about the Kremlin's desire to meddle with American democratic processes. This, in turn, has ignited speculation over America's cybersecurity posture, and the potential ties that Kaspersky Lab has with the Kremlin. Namely, that the Russian government could use products manufactured by Kaspersky Lab as a medium for engaging in nefarious cyber campaigns against U.S. information systems—including those at several federal departments and agencies—that are purportedly protected by the company's products.[6] Adding to concern, the FBI sent agents to visit "at least a dozen employees of Kaspersky" in order to question them "about the company's operations as part of a counter-intelligence inquiry."[7]

Given the increasing prevalence of cybersecurity threats across the nation, the federal government's use of cybersecurity products manufactured by a firm with potential ties to the Russian government is concerning to Congress. In May, the Senate Intelligence Committee held an open hearing where several top U.S. intelligence officials stated with consensus that they would not be comfortable using Kaspersky Lab's products on their systems.[8] Additionally, on June 15, 2017, the House Science Committee Subcommittees on Oversight and Research and Technology held a joint hearing where cybersecurity experts testified on industry approaches and

---

[3] Carol Matlack, *The Company Securing Your Internet Has Close Ties to Russian Spies*, BLOOMBERG BUSINESSWEEK, Mar. 19, 2015, *available at* https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies (last visited June 19, 2017).

[4] Joseph Menn, *Exclusive: Russian Antivirus Firm Faked Malware to Harm Rivals*, REUTERS, Aug. 14, 2015, *available at* www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QJ1CR20150814 (last visited June 27, 2017); *see also* Joseph Menn, *Exclusive: Russia's Kaspersky Threatened to 'Rub Out' Rival, Email Shows*, REUTERS, Aug. 28, 2015, *available at* http://www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QX2GO20150828 (last visited June 27, 2017).

[5] *Id.*

[6] *See* Ali Watkins, *US Officials Are Warning About A Russian Cybersecurity Company's US Government Ties*, BUZZFEED NEWS, May 8, 2017, *available at* https://www.buzzfeed.com/alimwatkins/us-officials-are-warning-about-a-russian-cybersecurity?utm_term=.osyYrP2Mz6#.kexPnOw1Lk (last visited June 19, 2017); *see also* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).

[7] Ken Dilanian & Tom Winter, *Bill Would Bar Pentagon From Business With Russian Cyber Firm Kaspersky*, NBC NEWS, June 28, 2017, *available at* http://www.nbcnews.com/news/us-news/fbi-interviews-employees-russia-linked-cyber-security-firm-kaspersky-lab-n777571 (last visited June 29, 2017); *see also* Joe Uchill, *FBI Visits Kaspersky Lab Employees*, THE HILL, June 28, 2017, *available at* http://thehill.com/policy/cybersecurity/339887-fbi-visits-kaspersky-lab-employees (last visited June 29, 2017).

[8] S. Comm. on Intel., *Worldwide Threats Hearing*, 115th Cong. (May 11, 2017). (question and answer by Senator Marco Rubio).

best practices for safeguarding against future cyber threats.[9] Among the panel of expert witnesses was Salim Neino, CEO of Kryptos Logic—the cybersecurity firm whose employee helped thwart further propagation of the recent WannaCry ransomware attack.[10] In response to questions about the ability of a software manufacturer to embed a "backdoor" into anti-virus software—to facilitate a State's cyber-espionage activities—Mr. Neino alarmingly affirmed that he had "seen that a multitude of times" in the past, and that the barriers to engaging in such activities are "very low."[11] This revelation gives the Committee great concern, especially in light of the capabilities that anti-virus software possesses. Additionally, in response to a question regarding Kaspersky Lab, retired Army General Gregory Touhill, the first federal chief information security officer or CISO, told the Committee: "I buy American."[12]

Anti-virus software is extremely powerful and operates by scanning files at the system level, rather than on the network periphery.[13] As such, other security systems generally do not monitor the operations carried out by the anti-virus software.[14] From a practical perspective, this means that compromised anti-virus software could be used for malicious or nefarious purposes, and could do so without detection. If anti-virus technology or systems are compromised by a user's adversary, it could install malicious code disguised as a security update; it could forego specific updates to pave the way for use of certain vectors of attack; it could forego beneficial updates for a specified subset of users; and it could even extract data that a user's adversary considers valuable.[15] Furthermore, anti-virus is so powerful that it has nearly unimpeded access into all attachments, files, and information contained on a system.[16] In sum, compromised anti-virus has the potential to undermine the security and integrity of any system on which it is installed.

The security and integrity of federal information systems are only as strong as the products that guard them. Although Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, requires federal departments and agencies to implement the NIST Cybersecurity Framework and to provide reports related thereto,[17] the

---

[9] H. Comm. on Science, Space, & Tech. Subcomm. on Research & Tech. jointly with the Subcomm. on Oversight, *Hearing on Bolstering the Government's Cybersecurity: Lessons Learned from WannaCry*, Preliminary Hearing Transcript, 115th Cong. (June 15, 2017) at 61.
[10] *Id.*
[11] *Id.* at 62 (question and answer by Representative Clay Higgins).
[12] *Id.* at 63.
[13] *See* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] The White House, *Executive Order – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017), *available at* https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal (last visited June 29, 2017).

security of federal systems may nevertheless be undermined by compromised anti-virus products. Government contracting data indicating that several federal departments and agencies use or have used cybersecurity or anti-virus products manufactured by Kaspersky Lab is even more troubling.[18] If federal agencies and departments are being guarded by potentially compromised software, then it is virtually impossible for such agencies to effectively and efficiently implement the NIST Framework, and to fully comply with President Trump's executive order. The recent news that Kaspersky Lab's products have been removed from the General Service Administration's contracting Schedule 67 and 70 is encouraging, however federal agencies and contractors may be likely to continue use of Kaspersky Lab's products.[19]

Cybersecurity is a greater threat to our nation than ever before. If these widely reported allegations prove true, then the American public has ample grounds on which to rest their concerns about the security of data stored and transmitted on federal information systems—especially those allegedly protected by Kaspersky Lab's products. In light of this increasing threat, the Committee takes seriously its duty to ensure the NIST Cybersecurity Framework is properly equipped and adapted to safeguard our nation's information. To assist the Committee in understanding the effectiveness of the NIST Framework, and potential vulnerabilities that exist on federal information systems, please provide the following documents and information as soon as possible, but no later than August 11, 2017. Please provide the requested materials for the time frame from January 1, 2013, to present:

1. All documents and communications referring or relating to cybersecurity and/or anti-virus products manufactured by Kaspersky Lab.

2. All documents and communications referring or relating to any evaluation, risk assessment, and decision-making processes on the matter of whether to implement products manufactured by Kaspersky Lab.

3. All documents and communications referring or relating to the use or implementation of products manufactured by Kaspersky Lab.

---

[18] Government Contracting Dataset, *available at* https://www.usaspending.gov/Pages/AdvancedSearch.aspx?k=kaspersky (last visited June 29, 2017); *see* David Goldstein & Greg Gordon, *Exclusive: Kremlin Documents Suggest Link Between Cyber Giant and Russia Spy Agency*, MCCLATCHY, July 3, 2017, *available at* http://www.mcclatchydc.com/news/nation-world/national/article159342694.html (last visited July 12, 2017); *see also* Mike Levine & Pierre Thomas, *Officials Fear Russia Could Try To Target US Through Popular Software Firm Under FBI Scrutiny*, ABC NEWS, May 9, 2017, *available at* http://abcnews.go.com/US/officials-fear-russia-target-us-popular-software-firm/story?id=47295729 (last visited July 12, 2017).

[19] *See* Sarah Kuranda, *Kaspersky Lab Removed From GSA Schedule, Limiting Federal Sales for Its Security Software*, CRN, July 12, 2017, *available at* http://www.crn.com/news/security/300088591/kaspersky-removed-from-gsa-schedule-limiting-federal-sales-for-its-security-software.htm; *see also* Eric Geller, *Trump Administration Restricts Popular Russian Security Software*, POLITICO, July 11, 2017, *available at* http://www.politico.com/story/2017/07/11/trump-russian-security-software-240423.

4. A complete list of any computers, systems, data, media, and/or information utilizing or accessible to Kaspersky Lab products or services.

5. Identify any federal government contractors or subcontractors known to be utilizing Kaspersky Lab's products to fulfill requirements of contracts with the Department or Agency.

6. All documents and communications referring or relating to the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity.

7. All documents and communications referring or relating to the production of reports required by Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.

Pursuant to House Rule X, the Committee on Science, Space, and Technology has jurisdiction over National Institute of Standards and Technology which develops cybersecurity standards and guidelines for the federal government and recommendations for the private sector.

When producing documents to the Committee, please deliver production sets to the Majority Staff in Room 2321 of the Rayburn House Office Building and the Minority Staff in Room 394 of the Ford House Office Building. The Committee prefers, if possible, to receive all documents in electronic format.

If you have any questions about this request, please contact Drew Colliatie or Tom Connally at 202-225-6371. Thank you for your attention to this matter.

Sincerely,

Lamar Smith
Chairman

cc: The Honorable Eddie Bernice Johnson, Ranking Minority Member

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6301
(202) 225–6371
www.science.house.gov

July 27, 2017

The Honorable Betsy DeVos
Secretary
U.S. Department of Education
400 Maryland Avenue SW
Washington D.C. 20202

Dear Secretary DeVos,

As part of an ongoing review of the federal government's cybersecurity policies and standards, the Committee on Science, Space, and Technology is requesting information and documents from the Department regarding Kaspersky Lab. The Committee is charged with oversight of the National Institute of Standards and Technology (NIST), and continuously evaluates whether changes to the Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework) are necessary. The documents and information will assist the Committee in determining whether the Framework requires further refinement when implemented by federal departments and agencies.

Kaspersky Lab is among the world's largest cybersecurity companies. Headquartered in Moscow, Russia, it services approximately 400 million users worldwide, including a number of United States Government Agencies and entities.[1] Kaspersky Lab specializes in anti-virus software—products with potentially uninhibited access to the systems they protect.[2] Although Kaspersky Lab was once considered a reputable cybersecurity firm, several concerns have been raised regarding the company and Eugene Kaspersky—the founder and CEO of Kaspersky Lab—and his potential ties to the Russian government.

The Committee is concerned that Kaspersky Lab is susceptible to manipulation by the Russian government, and that its products could be used as a tool for espionage, sabotage, or other nefarious activities against the United States. As early as 2015, reports began to surface

---

[1] *See* Jordan Robertson, *A Russian Cybersecurity Company's Ties to the Kremlin*, BLOOMBERG GOVERNMENT, Jul. 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSXAKB6JIJVL (last visited July 11, 2017).
[2] *See* Jordan Robertson & Michael Riley, *Kaspersky Lab Has Been Working With Russian Intelligence*, BLOOMBERG GOVERNMENT, July 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSX50G6KLVR5 (last visited July 11, 2017).

alleging that Mr. Kaspersky may have "close ties to Russian spies."[3] Shortly thereafter, *Reuters* reported that Kaspersky Lab engaged in a "sabotage" campaign undoubtedly targeting the U.S. cybersecurity market.[4] Specifically, the company "tried to damage rivals in the marketplace by tricking their antivirus software programs into classifying benign files as malicious."[5] More recently, Russia's alleged interference in the 2016 presidential election has heightened public concerns about the Kremlin's desire to meddle with American democratic processes. This, in turn, has ignited speculation over America's cybersecurity posture, and the potential ties that Kaspersky Lab has with the Kremlin. Namely, that the Russian government could use products manufactured by Kaspersky Lab as a medium for engaging in nefarious cyber campaigns against U.S. information systems—including those at several federal departments and agencies—that are purportedly protected by the company's products.[6] Adding to concern, the FBI sent agents to visit "at least a dozen employees of Kaspersky" in order to question them "about the company's operations as part of a counter-intelligence inquiry."[7]

Given the increasing prevalence of cybersecurity threats across the nation, the federal government's use of cybersecurity products manufactured by a firm with potential ties to the Russian government is concerning to Congress. In May, the Senate Intelligence Committee held an open hearing where several top U.S. intelligence officials stated with consensus that they would not be comfortable using Kaspersky Lab's products on their systems.[8] Additionally, on June 15, 2017, the House Science Committee Subcommittees on Oversight and Research and Technology held a joint hearing where cybersecurity experts testified on industry approaches and

---

[3] Carol Matlack, *The Company Securing Your Internet Has Close Ties to Russian Spies*, BLOOMBERG BUSINESSWEEK, Mar. 19, 2015, *available at* https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies (last visited June 19, 2017).

[4] Joseph Menn, *Exclusive: Russian Antivirus Firm Faked Malware to Harm Rivals*, REUTERS, Aug. 14, 2015, *available at* www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QJ1CR20150814 (last visited June 27, 2017); *see also* Joseph Menn, *Exclusive: Russia's Kaspersky Threatened to 'Rub Out' Rival, Email Shows*, REUTERS, Aug. 28, 2015, *available at* http://www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QX2GO20150828 (last visited June 27, 2017).

[5] *Id.*

[6] *See* Ali Watkins, *US Officials Are Warning About A Russian Cybersecurity Company's US Government Ties*, BUZZFEED NEWS, May 8, 2017, *available at* https://www.buzzfeed.com/alimwatkins/us-officials-are-warning-about-a-russian-cybersecurity?utm_term=.osyYrP2Mz6#.kexPnOw1Lk (last visited June 19, 2017); *see also* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).

[7] Ken Dilanian & Tom Winter, *Bill Would Bar Pentagon From Business With Russian Cyber Firm Kaspersky*, NBC NEWS, June 28, 2017, *available at* http://www.nbcnews.com/news/us-news/fbi-interviews-employees-russia-linked-cyber-security-firm-kaspersky-lab-n777571 (last visited June 29, 2017); *see also* Joe Uchill, *FBI Visits Kaspersky Lab Employees*, THE HILL, June 28, 2017, *available at* http://thehill.com/policy/cybersecurity/339887-fbi-visits-kaspersky-lab-employees (last visited June 29, 2017).

[8] S. Comm. on Intel., *Worldwide Threats Hearing*, 115th Cong. (May 11, 2017). (question and answer by Senator Marco Rubio).

best practices for safeguarding against future cyber threats.[9] Among the panel of expert witnesses was Salim Neino, CEO of Kryptos Logic—the cybersecurity firm whose employee helped thwart further propagation of the recent WannaCry ransomware attack.[10] In response to questions about the ability of a software manufacturer to embed a "backdoor" into anti-virus software—to facilitate a State's cyber-espionage activities—Mr. Neino alarmingly affirmed that he had "seen that a multitude of times" in the past, and that the barriers to engaging in such activities are "very low."[11] This revelation gives the Committee great concern, especially in light of the capabilities that anti-virus software possesses. Additionally, in response to a question regarding Kaspersky Lab, retired Army General Gregory Touhill, the first federal chief information security officer or CISO, told the Committee: "I buy American."[12]

Anti-virus software is extremely powerful and operates by scanning files at the system level, rather than on the network periphery.[13] As such, other security systems generally do not monitor the operations carried out by the anti-virus software.[14] From a practical perspective, this means that compromised anti-virus software could be used for malicious or nefarious purposes, and could do so without detection. If anti-virus technology or systems are compromised by a user's adversary, it could install malicious code disguised as a security update; it could forego specific updates to pave the way for use of certain vectors of attack; it could forego beneficial updates for a specified subset of users; and it could even extract data that a user's adversary considers valuable.[15] Furthermore, anti-virus is so powerful that it has nearly unimpeded access into all attachments, files, and information contained on a system.[16] In sum, compromised anti-virus has the potential to undermine the security and integrity of any system on which it is installed.

The security and integrity of federal information systems are only as strong as the products that guard them. Although Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, requires federal departments and agencies to implement the NIST Cybersecurity Framework and to provide reports related thereto,[17] the

---

[9] H. Comm. on Science, Space, & Tech. Subcomm. on Research & Tech. jointly with the Subcomm. on Oversight, *Hearing on Bolstering the Government's Cybersecurity: Lessons Learned from WannaCry*, Preliminary Hearing Transcript, 115th Cong. (June 15, 2017) at 61.
[10] *Id.*
[11] *Id.* at 62 (question and answer by Representative Clay Higgins).
[12] *Id.* at 63.
[13] *See* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] The White House, *Executive Order – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017), *available at* https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal (last visited June 29, 2017).

security of federal systems may nevertheless be undermined by compromised anti-virus products. Government contracting data indicating that several federal departments and agencies use or have used cybersecurity or anti-virus products manufactured by Kaspersky Lab is even more troubling.[18] If federal agencies and departments are being guarded by potentially compromised software, then it is virtually impossible for such agencies to effectively and efficiently implement the NIST Framework, and to fully comply with President Trump's executive order. The recent news that Kaspersky Lab's products have been removed from the General Service Administration's contracting Schedule 67 and 70 is encouraging, however federal agencies and contractors may be likely to continue use of Kaspersky Lab's products.[19]

Cybersecurity is a greater threat to our nation than ever before. If these widely reported allegations prove true, then the American public has ample grounds on which to rest their concerns about the security of data stored and transmitted on federal information systems—especially those allegedly protected by Kaspersky Lab's products. In light of this increasing threat, the Committee takes seriously its duty to ensure the NIST Cybersecurity Framework is properly equipped and adapted to safeguard our nation's information. To assist the Committee in understanding the effectiveness of the NIST Framework, and potential vulnerabilities that exist on federal information systems, please provide the following documents and information as soon as possible, but no later than August 11, 2017. Please provide the requested materials for the time frame from January 1, 2013, to present:

1. All documents and communications referring or relating to cybersecurity and/or anti-virus products manufactured by Kaspersky Lab.

2. All documents and communications referring or relating to any evaluation, risk assessment, and decision-making processes on the matter of whether to implement products manufactured by Kaspersky Lab.

3. All documents and communications referring or relating to the use or implementation of products manufactured by Kaspersky Lab.

---

[18] Government Contracting Dataset, *available at* https://www.usaspending.gov/Pages/AdvancedSearch.aspx?k=kaspersky (last visited June 29, 2017); *see* David Goldstein & Greg Gordon, *Exclusive: Kremlin Documents Suggest Link Between Cyber Giant and Russia Spy Agency*, MCCLATCHY, July 3, 2017, *available at* http://www.mcclatchydc.com/news/nation-world/national/article159342694.html (last visited July 12, 2017); *see also* Mike Levine & Pierre Thomas, *Officials Fear Russia Could Try To Target US Through Popular Software Firm Under FBI Scrutiny*, ABC NEWS, May 9, 2017, *available at* http://abcnews.go.com/US/officials-fear-russia-target-us-popular-software-firm/story?id=47295729 (last visited July 12, 2017).

[19] *See* Sarah Kuranda, *Kaspersky Lab Removed From GSA Schedule, Limiting Federal Sales for Its Security Software*, CRN, July 12, 2017, *available at* http://www.crn.com/news/security/300088591/kaspersky-removed-from-gsa-schedule-limiting-federal-sales-for-its-security-software.htm; *see also* Eric Geller, *Trump Administration Restricts Popular Russian Security Software*, POLITICO, July 11, 2017, *available at* http://www.politico.com/story/2017/07/11/trump-russian-security-software-240423.

4. A complete list of any computers, systems, data, media, and/or information utilizing or accessible to Kaspersky Lab products or services.

5. Identify any federal government contractors or subcontractors known to be utilizing Kaspersky Lab's products to fulfill requirements of contracts with the Department or Agency.

6. All documents and communications referring or relating to the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity.

7. All documents and communications referring or relating to the production of reports required by Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.

Pursuant to House Rule X, the Committee on Science, Space, and Technology has jurisdiction over National Institute of Standards and Technology which develops cybersecurity standards and guidelines for the federal government and recommendations for the private sector.

When producing documents to the Committee, please deliver production sets to the Majority Staff in Room 2321 of the Rayburn House Office Building and the Minority Staff in Room 394 of the Ford House Office Building. The Committee prefers, if possible, to receive all documents in electronic format.

If you have any questions about this request, please contact Drew Colliatie or Tom Connally at 202-225-6371. Thank you for your attention to this matter.

Sincerely,

Lamar Smith
Chairman

cc: The Honorable Eddie Bernice Johnson, Ranking Minority Member

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6301
(202) 225–6371
www.science.house.gov

July 27, 2017

The Honorable Scott Pruitt
Administrator
U.S. Environmental Protection Agency
1200 Pennsylvania Ave NW
Washington D.C. 20460

Dear Administrator Pruitt,

As part of an ongoing review of the federal government's cybersecurity policies and standards, the Committee on Science, Space, and Technology is requesting information and documents from the Agency regarding Kaspersky Lab. The Committee is charged with oversight of the National Institute of Standards and Technology (NIST), and continuously evaluates whether changes to the Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework) are necessary. The documents and information will assist the Committee in determining whether the Framework requires further refinement when implemented by federal departments and agencies.

Kaspersky Lab is among the world's largest cybersecurity companies. Headquartered in Moscow, Russia, it services approximately 400 million users worldwide, including a number of United States Government Agencies and entities.[1] Kaspersky Lab specializes in anti-virus software—products with potentially uninhibited access to the systems they protect.[2] Although Kaspersky Lab was once considered a reputable cybersecurity firm, several concerns have been raised regarding the company and Eugene Kaspersky—the founder and CEO of Kaspersky Lab—and his potential ties to the Russian government.

The Committee is concerned that Kaspersky Lab is susceptible to manipulation by the Russian government, and that its products could be used as a tool for espionage, sabotage, or other nefarious activities against the United States. As early as 2015, reports began to surface

---

[1] *See* Jordan Robertson, *A Russian Cybersecurity Company's Ties to the Kremlin*, BLOOMBERG GOVERNMENT, Jul. 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSXAKB6JIJVL (last visited July 11, 2017).
[2] *See* Jordan Robertson & Michael Riley, *Kaspersky Lab Has Been Working With Russian Intelligence*, BLOOMBERG GOVERNMENT, July 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSX50G6KLVR5 (last visited July 11, 2017).

alleging that Mr. Kaspersky may have "close ties to Russian spies."[3] Shortly thereafter, *Reuters* reported that Kaspersky Lab engaged in a "sabotage" campaign undoubtedly targeting the U.S. cybersecurity market.[4] Specifically, the company "tried to damage rivals in the marketplace by tricking their antivirus software programs into classifying benign files as malicious."[5] More recently, Russia's alleged interference in the 2016 presidential election has heightened public concerns about the Kremlin's desire to meddle with American democratic processes. This, in turn, has ignited speculation over America's cybersecurity posture, and the potential ties that Kaspersky Lab has with the Kremlin. Namely, that the Russian government could use products manufactured by Kaspersky Lab as a medium for engaging in nefarious cyber campaigns against U.S. information systems—including those at several federal departments and agencies—that are purportedly protected by the company's products.[6] Adding to concern, the FBI sent agents to visit "at least a dozen employees of Kaspersky" in order to question them "about the company's operations as part of a counter-intelligence inquiry."[7]

Given the increasing prevalence of cybersecurity threats across the nation, the federal government's use of cybersecurity products manufactured by a firm with potential ties to the Russian government is concerning to Congress. In May, the Senate Intelligence Committee held an open hearing where several top U.S. intelligence officials stated with consensus that they would not be comfortable using Kaspersky Lab's products on their systems.[8] Additionally, on June 15, 2017, the House Science Committee Subcommittees on Oversight and Research and Technology held a joint hearing where cybersecurity experts testified on industry approaches and

---

[3] Carol Matlack, *The Company Securing Your Internet Has Close Ties to Russian Spies*, BLOOMBERG BUSINESSWEEK, Mar. 19, 2015, *available at* https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies (last visited June 19, 2017).

[4] Joseph Menn, *Exclusive: Russian Antivirus Firm Faked Malware to Harm Rivals*, REUTERS, Aug. 14, 2015, *available at* www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QJ1CR20150814 (last visited June 27, 2017); *see also* Joseph Menn, *Exclusive: Russia's Kaspersky Threatened to 'Rub Out' Rival, Email Shows*, REUTERS, Aug. 28, 2015, *available at* http://www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QX2GO20150828 (last visited June 27, 2017).

[5] *Id.*

[6] *See* Ali Watkins, *US Officials Are Warning About A Russian Cybersecurity Company's US Government Ties*, BUZZFEED NEWS, May 8, 2017, *available at* https://www.buzzfeed.com/alimwatkins/us-officials-are-warning-about-a-russian-cybersecurity?utm_term=.osyYrP2Mz6#.kexPnOw1Lk (last visited June 19, 2017); *see also* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).

[7] Ken Dilanian & Tom Winter, *Bill Would Bar Pentagon From Business With Russian Cyber Firm Kaspersky*, NBC NEWS, June 28, 2017, *available at* http://www.nbcnews.com/news/us-news/fbi-interviews-employees-russia-linked-cyber-security-firm-kaspersky-lab-n777571 (last visited June 29, 2017); *see also* Joe Uchill, *FBI Visits Kaspersky Lab Employees*, THE HILL, June 28, 2017, *available at* http://thehill.com/policy/cybersecurity/339887-fbi-visits-kaspersky-lab-employees (last visited June 29, 2017).

[8] S. Comm. on Intel., *Worldwide Threats Hearing*, 115th Cong. (May 11, 2017). (question and answer by Senator Marco Rubio).

best practices for safeguarding against future cyber threats.[9] Among the panel of expert witnesses was Salim Neino, CEO of Kryptos Logic—the cybersecurity firm whose employee helped thwart further propagation of the recent WannaCry ransomware attack.[10] In response to questions about the ability of a software manufacturer to embed a "backdoor" into anti-virus software—to facilitate a State's cyber-espionage activities—Mr. Neino alarmingly affirmed that he had "seen that a multitude of times" in the past, and that the barriers to engaging in such activities are "very low."[11] This revelation gives the Committee great concern, especially in light of the capabilities that anti-virus software possesses. Additionally, in response to a question regarding Kaspersky Lab, retired Army General Gregory Touhill, the first federal chief information security officer or CISO, told the Committee: "I buy American."[12]

Anti-virus software is extremely powerful and operates by scanning files at the system level, rather than on the network periphery.[13] As such, other security systems generally do not monitor the operations carried out by the anti-virus software.[14] From a practical perspective, this means that compromised anti-virus software could be used for malicious or nefarious purposes, and could do so without detection. If anti-virus technology or systems are compromised by a user's adversary, it could install malicious code disguised as a security update; it could forego specific updates to pave the way for use of certain vectors of attack; it could forego beneficial updates for a specified subset of users; and it could even extract data that a user's adversary considers valuable.[15] Furthermore, anti-virus is so powerful that it has nearly unimpeded access into all attachments, files, and information contained on a system.[16] In sum, compromised anti-virus has the potential to undermine the security and integrity of any system on which it is installed.

The security and integrity of federal information systems are only as strong as the products that guard them. Although Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, requires federal departments and agencies to implement the NIST Cybersecurity Framework and to provide reports related thereto,[17] the

---

[9] H. Comm. on Science, Space, & Tech. Subcomm. on Research & Tech. jointly with the Subcomm. on Oversight, *Hearing on Bolstering the Government's Cybersecurity: Lessons Learned from WannaCry*, Preliminary Hearing Transcript, 115th Cong. (June 15, 2017) at 61.
[10] *Id.*
[11] *Id.* at 62 (question and answer by Representative Clay Higgins).
[12] *Id.* at 63.
[13] *See* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] The White House, *Executive Order – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017), *available at* https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal (last visited June 29, 2017).

security of federal systems may nevertheless be undermined by compromised anti-virus products. Government contracting data indicating that several federal departments and agencies use or have used cybersecurity or anti-virus products manufactured by Kaspersky Lab is even more troubling.[18] If federal agencies and departments are being guarded by potentially compromised software, then it is virtually impossible for such agencies to effectively and efficiently implement the NIST Framework, and to fully comply with President Trump's executive order. The recent news that Kaspersky Lab's products have been removed from the General Service Administration's contracting Schedule 67 and 70 is encouraging, however federal agencies and contractors may be likely to continue use of Kaspersky Lab's products.[19]

Cybersecurity is a greater threat to our nation than ever before. If these widely reported allegations prove true, then the American public has ample grounds on which to rest their concerns about the security of data stored and transmitted on federal information systems—especially those allegedly protected by Kaspersky Lab's products. In light of this increasing threat, the Committee takes seriously its duty to ensure the NIST Cybersecurity Framework is properly equipped and adapted to safeguard our nation's information. To assist the Committee in understanding the effectiveness of the NIST Framework, and potential vulnerabilities that exist on federal information systems, please provide the following documents and information as soon as possible, but no later than August 11, 2017. Please provide the requested materials for the time frame from January 1, 2013, to present:

1. All documents and communications referring or relating to cybersecurity and/or anti-virus products manufactured by Kaspersky Lab.

2. All documents and communications referring or relating to any evaluation, risk assessment, and decision-making processes on the matter of whether to implement products manufactured by Kaspersky Lab.

3. All documents and communications referring or relating to the use or implementation of products manufactured by Kaspersky Lab.

---

[18] Government Contracting Dataset, *available at* https://www.usaspending.gov/Pages/AdvancedSearch.aspx?k=kaspersky (last visited June 29, 2017); *see* David Goldstein & Greg Gordon, *Exclusive: Kremlin Documents Suggest Link Between Cyber Giant and Russia Spy Agency*, MCCLATCHY, July 3, 2017, *available at* http://www.mcclatchydc.com/news/nation-world/national/article159342694.html (last visited July 12, 2017); *see also* Mike Levine & Pierre Thomas, *Officials Fear Russia Could Try To Target US Through Popular Software Firm Under FBI Scrutiny*, ABC NEWS, May 9, 2017, *available at* http://abcnews.go.com/US/officials-fear-russia-target-us-popular-software-firm/story?id=47295729 (last visited July 12, 2017).

[19] *See* Sarah Kuranda, *Kaspersky Lab Removed From GSA Schedule, Limiting Federal Sales for Its Security Software*, CRN, July 12, 2017, *available at* http://www.crn.com/news/security/300088591/kaspersky-removed-from-gsa-schedule-limiting-federal-sales-for-its-security-software.htm; *see also* Eric Geller, *Trump Administration Restricts Popular Russian Security Software*, POLITICO, July 11, 2017, *available at* http://www.politico.com/story/2017/07/11/trump-russian-security-software-240423.

4. A complete list of any computers, systems, data, media, and/or information utilizing or accessible to Kaspersky Lab products or services.

5. Identify any federal government contractors or subcontractors known to be utilizing Kaspersky Lab's products to fulfill requirements of contracts with the Department or Agency.

6. All documents and communications referring or relating to the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity.

7. All documents and communications referring or relating to the production of reports required by Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.

Pursuant to House Rule X, the Committee on Science, Space, and Technology has jurisdiction over National Institute of Standards and Technology which develops cybersecurity standards and guidelines for the federal government and recommendations for the private sector.

When producing documents to the Committee, please deliver production sets to the Majority Staff in Room 2321 of the Rayburn House Office Building and the Minority Staff in Room 394 of the Ford House Office Building. The Committee prefers, if possible, to receive all documents in electronic format.

If you have any questions about this request, please contact Drew Colliatie or Tom Connally at 202-225-6371. Thank you for your attention to this matter.

Sincerely,

Lamar Smith

Lamar Smith
Chairman

cc: The Honorable Eddie Bernice Johnson, Ranking Minority Member

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6301
(202) 225-6371
www.science.house.gov

July 27, 2017

The Honorable Thomas E. Price, M.D.
Secretary
U.S. Department of Health and Human Services
64 New York Avenue NE
Washington D.C. 20002

Dear Secretary Price,

As part of an ongoing review of the federal government's cybersecurity policies and standards, the Committee on Science, Space, and Technology is requesting information and documents from the Department regarding Kaspersky Lab. The Committee is charged with oversight of the National Institute of Standards and Technology (NIST), and continuously evaluates whether changes to the Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework) are necessary. The documents and information will assist the Committee in determining whether the Framework requires further refinement when implemented by federal departments and agencies.

Kaspersky Lab is among the world's largest cybersecurity companies. Headquartered in Moscow, Russia, it services approximately 400 million users worldwide, including a number of United States Government Agencies and entities.[1] Kaspersky Lab specializes in anti-virus software—products with potentially uninhibited access to the systems they protect.[2] Although Kaspersky Lab was once considered a reputable cybersecurity firm, several concerns have been raised regarding the company and Eugene Kaspersky—the founder and CEO of Kaspersky Lab—and his potential ties to the Russian government.

The Committee is concerned that Kaspersky Lab is susceptible to manipulation by the Russian government, and that its products could be used as a tool for espionage, sabotage, or other nefarious activities against the United States. As early as 2015, reports began to surface

---

[1] *See* Jordan Robertson, *A Russian Cybersecurity Company's Ties to the Kremlin*, BLOOMBERG GOVERNMENT, Jul. 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSXAKB6JIJVL (last visited July 11, 2017).
[2] *See* Jordan Robertson & Michael Riley, *Kaspersky Lab Has Been Working With Russian Intelligence*, BLOOMBERG GOVERNMENT, July 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSX50G6KLVR5 (last visited July 11, 2017).

alleging that Mr. Kaspersky may have "close ties to Russian spies."[3] Shortly thereafter, *Reuters* reported that Kaspersky Lab engaged in a "sabotage" campaign undoubtedly targeting the U.S. cybersecurity market.[4] Specifically, the company "tried to damage rivals in the marketplace by tricking their antivirus software programs into classifying benign files as malicious."[5] More recently, Russia's alleged interference in the 2016 presidential election has heightened public concerns about the Kremlin's desire to meddle with American democratic processes. This, in turn, has ignited speculation over America's cybersecurity posture, and the potential ties that Kaspersky Lab has with the Kremlin. Namely, that the Russian government could use products manufactured by Kaspersky Lab as a medium for engaging in nefarious cyber campaigns against U.S. information systems—including those at several federal departments and agencies—that are purportedly protected by the company's products.[6] Adding to concern, the FBI sent agents to visit "at least a dozen employees of Kaspersky" in order to question them "about the company's operations as part of a counter-intelligence inquiry."[7]

Given the increasing prevalence of cybersecurity threats across the nation, the federal government's use of cybersecurity products manufactured by a firm with potential ties to the Russian government is concerning to Congress. In May, the Senate Intelligence Committee held an open hearing where several top U.S. intelligence officials stated with consensus that they would not be comfortable using Kaspersky Lab's products on their systems.[8] Additionally, on June 15, 2017, the House Science Committee Subcommittees on Oversight and Research and Technology held a joint hearing where cybersecurity experts testified on industry approaches and

---

[3] Carol Matlack, *The Company Securing Your Internet Has Close Ties to Russian Spies*, BLOOMBERG BUSINESSWEEK, Mar. 19, 2015, *available at* https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies (last visited June 19, 2017).

[4] Joseph Menn, *Exclusive: Russian Antivirus Firm Faked Malware to Harm Rivals*, REUTERS, Aug. 14, 2015, *available at* www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QJ1CR20150814 (last visited June 27, 2017); *see also* Joseph Menn, *Exclusive: Russia's Kaspersky Threatened to 'Rub Out' Rival, Email Shows*, REUTERS, Aug. 28, 2015, *available at* http://www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QX2GO20150828 (last visited June 27, 2017).

[5] *Id.*

[6] *See* Ali Watkins, *US Officials Are Warning About A Russian Cybersecurity Company's US Government Ties*, BUZZFEED NEWS, May 8, 2017, *available at* https://www.buzzfeed.com/alimwatkins/us-officials-are-warning-about-a-russian-cybersecurity?utm_term=.osyYrP2Mz6#.kexPnOw1Lk (last visited June 19, 2017); *see also* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).

[7] Ken Dilanian & Tom Winter, *Bill Would Bar Pentagon From Business With Russian Cyber Firm Kaspersky*, NBC NEWS, June 28, 2017, *available at* http://www.nbcnews.com/news/us-news/fbi-interviews-employees-russia-linked-cyber-security-firm-kaspersky-lab-n777571 (last visited June 29, 2017); *see also* Joe Uchill, *FBI Visits Kaspersky Lab Employees*, THE HILL, June 28, 2017, *available at* http://thehill.com/policy/cybersecurity/339887-fbi-visits-kaspersky-lab-employees (last visited June 29, 2017).

[8] S. Comm. on Intel., *Worldwide Threats Hearing*, 115th Cong. (May 11, 2017). (question and answer by Senator Marco Rubio).

best practices for safeguarding against future cyber threats.[9] Among the panel of expert witnesses was Salim Neino, CEO of Kryptos Logic—the cybersecurity firm whose employee helped thwart further propagation of the recent WannaCry ransomware attack.[10] In response to questions about the ability of a software manufacturer to embed a "backdoor" into anti-virus software—to facilitate a State's cyber-espionage activities—Mr. Neino alarmingly affirmed that he had "seen that a multitude of times" in the past, and that the barriers to engaging in such activities are "very low."[11] This revelation gives the Committee great concern, especially in light of the capabilities that anti-virus software possesses. Additionally, in response to a question regarding Kaspersky Lab, retired Army General Gregory Touhill, the first federal chief information security officer or CISO, told the Committee: "I buy American."[12]

Anti-virus software is extremely powerful and operates by scanning files at the system level, rather than on the network periphery.[13] As such, other security systems generally do not monitor the operations carried out by the anti-virus software.[14] From a practical perspective, this means that compromised anti-virus software could be used for malicious or nefarious purposes, and could do so without detection. If anti-virus technology or systems are compromised by a user's adversary, it could install malicious code disguised as a security update; it could forego specific updates to pave the way for use of certain vectors of attack; it could forego beneficial updates for a specified subset of users; and it could even extract data that a user's adversary considers valuable.[15] Furthermore, anti-virus is so powerful that it has nearly unimpeded access into all attachments, files, and information contained on a system.[16] In sum, compromised anti-virus has the potential to undermine the security and integrity of any system on which it is installed.

The security and integrity of federal information systems are only as strong as the products that guard them. Although Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, requires federal departments and agencies to implement the NIST Cybersecurity Framework and to provide reports related thereto,[17] the

---

[9] H. Comm. on Science, Space, & Tech. Subcomm. on Research & Tech. jointly with the Subcomm. on Oversight, *Hearing on Bolstering the Government's Cybersecurity: Lessons Learned from WannaCry*, Preliminary Hearing Transcript, 115th Cong. (June 15, 2017) at 61.

[10] *Id.*

[11] *Id.* at 62 (question and answer by Representative Clay Higgins).

[12] *Id.* at 63.

[13] *See* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).

[14] *Id.*

[15] *Id.*

[16] *Id.*

[17] The White House, *Executive Order – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017), *available at* https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal (last visited June 29, 2017).

security of federal systems may nevertheless be undermined by compromised anti-virus products. Government contracting data indicating that several federal departments and agencies use or have used cybersecurity or anti-virus products manufactured by Kaspersky Lab is even more troubling.[18] If federal agencies and departments are being guarded by potentially compromised software, then it is virtually impossible for such agencies to effectively and efficiently implement the NIST Framework, and to fully comply with President Trump's executive order. The recent news that Kaspersky Lab's products have been removed from the General Service Administration's contracting Schedule 67 and 70 is encouraging, however federal agencies and contractors may be likely to continue use of Kaspersky Lab's products.[19]

Cybersecurity is a greater threat to our nation than ever before. If these widely reported allegations prove true, then the American public has ample grounds on which to rest their concerns about the security of data stored and transmitted on federal information systems—especially those allegedly protected by Kaspersky Lab's products. In light of this increasing threat, the Committee takes seriously its duty to ensure the NIST Cybersecurity Framework is properly equipped and adapted to safeguard our nation's information. To assist the Committee in understanding the effectiveness of the NIST Framework, and potential vulnerabilities that exist on federal information systems, please provide the following documents and information as soon as possible, but no later than August 11, 2017. Please provide the requested materials for the time frame from January 1, 2013, to present:

1. All documents and communications referring or relating to cybersecurity and/or anti-virus products manufactured by Kaspersky Lab.

2. All documents and communications referring or relating to any evaluation, risk assessment, and decision-making processes on the matter of whether to implement products manufactured by Kaspersky Lab.

3. All documents and communications referring or relating to the use or implementation of products manufactured by Kaspersky Lab.

---

[18] Government Contracting Dataset, *available at* https://www.usaspending.gov/Pages/AdvancedSearch.aspx?k=kaspersky (last visited June 29, 2017); *see* David Goldstein & Greg Gordon, *Exclusive: Kremlin Documents Suggest Link Between Cyber Giant and Russia Spy Agency*, MCCLATCHY, July 3, 2017, *available at* http://www.mcclatchydc.com/news/nation-world/national/article159342694.html (last visited July 12, 2017); *see also* Mike Levine & Pierre Thomas, *Officials Fear Russia Could Try To Target US Through Popular Software Firm Under FBI Scrutiny*, ABC NEWS, May 9, 2017, *available at* http://abcnews.go.com/US/officials-fear-russia-target-us-popular-software-firm/story?id=47295729 (last visited July 12, 2017).

[19] *See* Sarah Kuranda, *Kaspersky Lab Removed From GSA Schedule, Limiting Federal Sales for Its Security Software*, CRN, July 12, 2017, *available at* http://www.crn.com/news/security/300088591/kaspersky-removed-from-gsa-schedule-limiting-federal-sales-for-its-security-software.htm; *see also* Eric Geller, *Trump Administration Restricts Popular Russian Security Software*, POLITICO, July 11, 2017, *available at* http://www.politico.com/story/2017/07/11/trump-russian-security-software-240423.

4. A complete list of any computers, systems, data, media, and/or information utilizing or accessible to Kaspersky Lab products or services.

5. Identify any federal government contractors or subcontractors known to be utilizing Kaspersky Lab's products to fulfill requirements of contracts with the Department or Agency.

6. All documents and communications referring or relating to the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity.

7. All documents and communications referring or relating to the production of reports required by Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.

Pursuant to House Rule X, the Committee on Science, Space, and Technology has jurisdiction over National Institute of Standards and Technology which develops cybersecurity standards and guidelines for the federal government and recommendations for the private sector.

When producing documents to the Committee, please deliver production sets to the Majority Staff in Room 2321 of the Rayburn House Office Building and the Minority Staff in Room 394 of the Ford House Office Building. The Committee prefers, if possible, to receive all documents in electronic format.

If you have any questions about this request, please contact Drew Colliatie or Tom Connally at 202-225-6371. Thank you for your attention to this matter.

Sincerely,

Lamar Smith
Chairman

cc: The Honorable Eddie Bernice Johnson, Ranking Minority Member

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6301
(202) 225–6371
www.science.house.gov

July 27, 2017

The Honorable Ben Carson
Secretary
U.S. Department of Housing and Urban Development
451 7th Street SW
Washington D.C. 20410

Dear Secretary Carson,

As part of an ongoing review of the federal government's cybersecurity policies and standards, the Committee on Science, Space, and Technology is requesting information and documents from the Department regarding Kaspersky Lab. The Committee is charged with oversight of the National Institute of Standards and Technology (NIST), and continuously evaluates whether changes to the Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework) are necessary. The documents and information will assist the Committee in determining whether the Framework requires further refinement when implemented by federal departments and agencies.

Kaspersky Lab is among the world's largest cybersecurity companies. Headquartered in Moscow, Russia, it services approximately 400 million users worldwide, including a number of United States Government Agencies and entities.[1] Kaspersky Lab specializes in anti-virus software—products with potentially uninhibited access to the systems they protect.[2] Although Kaspersky Lab was once considered a reputable cybersecurity firm, several concerns have been raised regarding the company and Eugene Kaspersky—the founder and CEO of Kaspersky Lab—and his potential ties to the Russian government.

The Committee is concerned that Kaspersky Lab is susceptible to manipulation by the Russian government, and that its products could be used as a tool for espionage, sabotage, or other nefarious activities against the United States. As early as 2015, reports began to surface

---

[1] *See* Jordan Robertson, *A Russian Cybersecurity Company's Ties to the Kremlin*, BLOOMBERG GOVERNMENT, Jul. 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSXAKB6JIJVL (last visited July 11, 2017).
[2] *See* Jordan Robertson & Michael Riley, *Kaspersky Lab Has Been Working With Russian Intelligence*, BLOOMBERG GOVERNMENT, July 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSX50G6KLVR5 (last visited July 11, 2017).

alleging that Mr. Kaspersky may have "close ties to Russian spies."[3] Shortly thereafter, *Reuters* reported that Kaspersky Lab engaged in a "sabotage" campaign undoubtedly targeting the U.S. cybersecurity market.[4] Specifically, the company "tried to damage rivals in the marketplace by tricking their antivirus software programs into classifying benign files as malicious."[5] More recently, Russia's alleged interference in the 2016 presidential election has heightened public concerns about the Kremlin's desire to meddle with American democratic processes. This, in turn, has ignited speculation over America's cybersecurity posture, and the potential ties that Kaspersky Lab has with the Kremlin. Namely, that the Russian government could use products manufactured by Kaspersky Lab as a medium for engaging in nefarious cyber campaigns against U.S. information systems—including those at several federal departments and agencies—that are purportedly protected by the company's products.[6] Adding to concern, the FBI sent agents to visit "at least a dozen employees of Kaspersky" in order to question them "about the company's operations as part of a counter-intelligence inquiry."[7]

Given the increasing prevalence of cybersecurity threats across the nation, the federal government's use of cybersecurity products manufactured by a firm with potential ties to the Russian government is concerning to Congress. In May, the Senate Intelligence Committee held an open hearing where several top U.S. intelligence officials stated with consensus that they would not be comfortable using Kaspersky Lab's products on their systems.[8] Additionally, on June 15, 2017, the House Science Committee Subcommittees on Oversight and Research and Technology held a joint hearing where cybersecurity experts testified on industry approaches and

---

[3] Carol Matlack, *The Company Securing Your Internet Has Close Ties to Russian Spies*, BLOOMBERG BUSINESSWEEK, Mar. 19, 2015, *available at* https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies (last visited June 19, 2017).

[4] Joseph Menn, *Exclusive: Russian Antivirus Firm Faked Malware to Harm Rivals*, REUTERS, Aug. 14, 2015, *available at* www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QJ1CR20150814 (last visited June 27, 2017); *see also* Joseph Menn, *Exclusive: Russia's Kaspersky Threatened to 'Rub Out' Rival, Email Shows*, REUTERS, Aug. 28, 2015, *available at* http://www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QX2GO20150828 (last visited June 27, 2017).

[5] *Id.*

[6] *See* Ali Watkins, *US Officials Are Warning About A Russian Cybersecurity Company's US Government Ties*, BUZZFEED NEWS, May 8, 2017, *available at* https://www.buzzfeed.com/alimwatkins/us-officials-are-warning-about-a-russian-cybersecurity?utm_term=.osyYrP2Mz6#.kexPnOw1Lk (last visited June 19, 2017); *see also* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).

[7] Ken Dilanian & Tom Winter, *Bill Would Bar Pentagon From Business With Russian Cyber Firm Kaspersky*, NBC NEWS, June 28, 2017, *available at* http://www.nbcnews.com/news/us-news/fbi-interviews-employees-russia-linked-cyber-security-firm-kaspersky-lab-n777571 (last visited June 29, 2017); *see also* Joe Uchill, *FBI Visits Kaspersky Lab Employees*, THE HILL, June 28, 2017, *available at* http://thehill.com/policy/cybersecurity/339887-fbi-visits-kaspersky-lab-employees (last visited June 29, 2017).

[8] S. Comm. on Intel., *Worldwide Threats Hearing*, 115th Cong. (May 11, 2017). (question and answer by Senator Marco Rubio).

best practices for safeguarding against future cyber threats.[9] Among the panel of expert witnesses was Salim Neino, CEO of Kryptos Logic—the cybersecurity firm whose employee helped thwart further propagation of the recent WannaCry ransomware attack.[10] In response to questions about the ability of a software manufacturer to embed a "backdoor" into anti-virus software—to facilitate a State's cyber-espionage activities—Mr. Neino alarmingly affirmed that he had "seen that a multitude of times" in the past, and that the barriers to engaging in such activities are "very low."[11] This revelation gives the Committee great concern, especially in light of the capabilities that anti-virus software possesses. Additionally, in response to a question regarding Kaspersky Lab, retired Army General Gregory Touhill, the first federal chief information security officer or CISO, told the Committee: "I buy American."[12]

Anti-virus software is extremely powerful and operates by scanning files at the system level, rather than on the network periphery.[13] As such, other security systems generally do not monitor the operations carried out by the anti-virus software.[14] From a practical perspective, this means that compromised anti-virus software could be used for malicious or nefarious purposes, and could do so without detection. If anti-virus technology or systems are compromised by a user's adversary, it could install malicious code disguised as a security update; it could forego specific updates to pave the way for use of certain vectors of attack; it could forego beneficial updates for a specified subset of users; and it could even extract data that a user's adversary considers valuable.[15] Furthermore, anti-virus is so powerful that it has nearly unimpeded access into all attachments, files, and information contained on a system.[16] In sum, compromised anti-virus has the potential to undermine the security and integrity of any system on which it is installed.

The security and integrity of federal information systems are only as strong as the products that guard them. Although Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, requires federal departments and agencies to implement the NIST Cybersecurity Framework and to provide reports related thereto,[17] the

---

[9] H. Comm. on Science, Space, & Tech. Subcomm. on Research & Tech. jointly with the Subcomm. on Oversight, *Hearing on Bolstering the Government's Cybersecurity: Lessons Learned from WannaCry*, Preliminary Hearing Transcript, 115th Cong. (June 15, 2017) at 61.
[10] *Id.*
[11] *Id.* at 62 (question and answer by Representative Clay Higgins).
[12] *Id.* at 63.
[13] *See* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] The White House, *Executive Order – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017), *available at* https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal (last visited June 29, 2017).

security of federal systems may nevertheless be undermined by compromised anti-virus products. Government contracting data indicating that several federal departments and agencies use or have used cybersecurity or anti-virus products manufactured by Kaspersky Lab is even more troubling.[18] If federal agencies and departments are being guarded by potentially compromised software, then it is virtually impossible for such agencies to effectively and efficiently implement the NIST Framework, and to fully comply with President Trump's executive order. The recent news that Kaspersky Lab's products have been removed from the General Service Administration's contracting Schedule 67 and 70 is encouraging, however federal agencies and contractors may be likely to continue use of Kaspersky Lab's products.[19]

Cybersecurity is a greater threat to our nation than ever before. If these widely reported allegations prove true, then the American public has ample grounds on which to rest their concerns about the security of data stored and transmitted on federal information systems—especially those allegedly protected by Kaspersky Lab's products. In light of this increasing threat, the Committee takes seriously its duty to ensure the NIST Cybersecurity Framework is properly equipped and adapted to safeguard our nation's information. To assist the Committee in understanding the effectiveness of the NIST Framework, and potential vulnerabilities that exist on federal information systems, please provide the following documents and information as soon as possible, but no later than August 11, 2017. Please provide the requested materials for the time frame from January 1, 2013, to present:

1. All documents and communications referring or relating to cybersecurity and/or anti-virus products manufactured by Kaspersky Lab.

2. All documents and communications referring or relating to any evaluation, risk assessment, and decision-making processes on the matter of whether to implement products manufactured by Kaspersky Lab.

3. All documents and communications referring or relating to the use or implementation of products manufactured by Kaspersky Lab.

---

[18] Government Contracting Dataset, *available at* https://www.usaspending.gov/Pages/AdvancedSearch.aspx?k=kaspersky (last visited June 29, 2017); *see* David Goldstein & Greg Gordon, *Exclusive: Kremlin Documents Suggest Link Between Cyber Giant and Russia Spy Agency*, MCCLATCHY, July 3, 2017, *available at* http://www.mcclatchydc.com/news/nation-world/national/article159342694.html (last visited July 12, 2017); *see also* Mike Levine & Pierre Thomas, *Officials Fear Russia Could Try To Target US Through Popular Software Firm Under FBI Scrutiny*, ABC NEWS, May 9, 2017, *available at* http://abcnews.go.com/US/officials-fear-russia-target-us-popular-software-firm/story?id=47295729 (last visited July 12, 2017).

[19] *See* Sarah Kuranda, *Kaspersky Lab Removed From GSA Schedule, Limiting Federal Sales for Its Security Software*, CRN, July 12, 2017, *available at* http://www.crn.com/news/security/300088591/kaspersky-removed-from-gsa-schedule-limiting-federal-sales-for-its-security-software.htm; *see also* Eric Geller, *Trump Administration Restricts Popular Russian Security Software*, POLITICO, July 11, 2017, *available at* http://www.politico.com/story/2017/07/11/trump-russian-security-software-240423.

4. A complete list of any computers, systems, data, media, and/or information utilizing or accessible to Kaspersky Lab products or services.

5. Identify any federal government contractors or subcontractors known to be utilizing Kaspersky Lab's products to fulfill requirements of contracts with the Department or Agency.

6. All documents and communications referring or relating to the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity.

7. All documents and communications referring or relating to the production of reports required by Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.

Pursuant to House Rule X, the Committee on Science, Space, and Technology has jurisdiction over National Institute of Standards and Technology which develops cybersecurity standards and guidelines for the federal government and recommendations for the private sector.

When producing documents to the Committee, please deliver production sets to the Majority Staff in Room 2321 of the Rayburn House Office Building and the Minority Staff in Room 394 of the Ford House Office Building. The Committee prefers, if possible, to receive all documents in electronic format.

If you have any questions about this request, please contact Drew Colliatie or Tom Connally at 202-225-6371. Thank you for your attention to this matter.

Sincerely,

Lamar Smith
Chairman

cc: The Honorable Eddie Bernice Johnson, Ranking Minority Member

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6301
(202) 225–6371
www.science.house.gov

July 27, 2017

The Honorable Ryan Zinke
Secretary
U.S. Department of Interior
1849 C Street NW
Washington D.C. 20240

Dear Secretary Zinke,

As part of an ongoing review of the federal government's cybersecurity policies and standards, the Committee on Science, Space, and Technology is requesting information and documents from the Department regarding Kaspersky Lab. The Committee is charged with oversight of the National Institute of Standards and Technology (NIST), and continuously evaluates whether changes to the Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework) are necessary. The documents and information will assist the Committee in determining whether the Framework requires further refinement when implemented by federal departments and agencies.

Kaspersky Lab is among the world's largest cybersecurity companies. Headquartered in Moscow, Russia, it services approximately 400 million users worldwide, including a number of United States Government Agencies and entities.[1] Kaspersky Lab specializes in anti-virus software—products with potentially uninhibited access to the systems they protect.[2] Although Kaspersky Lab was once considered a reputable cybersecurity firm, several concerns have been raised regarding the company and Eugene Kaspersky—the founder and CEO of Kaspersky Lab—and his potential ties to the Russian government.

The Committee is concerned that Kaspersky Lab is susceptible to manipulation by the Russian government, and that its products could be used as a tool for espionage, sabotage, or other nefarious activities against the United States. As early as 2015, reports began to surface

---

[1] *See* Jordan Robertson, *A Russian Cybersecurity Company's Ties to the Kremlin*, BLOOMBERG GOVERNMENT, Jul. 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSXAKB6JIJVL (last visited July 11, 2017).
[2] *See* Jordan Robertson & Michael Riley, *Kaspersky Lab Has Been Working With Russian Intelligence*, BLOOMBERG GOVERNMENT, July 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSX50G6KLVR5 (last visited July 11, 2017).

alleging that Mr. Kaspersky may have "close ties to Russian spies."[3] Shortly thereafter, *Reuters* reported that Kaspersky Lab engaged in a "sabotage" campaign undoubtedly targeting the U.S. cybersecurity market.[4] Specifically, the company "tried to damage rivals in the marketplace by tricking their antivirus software programs into classifying benign files as malicious."[5] More recently, Russia's alleged interference in the 2016 presidential election has heightened public concerns about the Kremlin's desire to meddle with American democratic processes. This, in turn, has ignited speculation over America's cybersecurity posture, and the potential ties that Kaspersky Lab has with the Kremlin. Namely, that the Russian government could use products manufactured by Kaspersky Lab as a medium for engaging in nefarious cyber campaigns against U.S. information systems—including those at several federal departments and agencies—that are purportedly protected by the company's products.[6] Adding to concern, the FBI sent agents to visit "at least a dozen employees of Kaspersky" in order to question them "about the company's operations as part of a counter-intelligence inquiry."[7]

Given the increasing prevalence of cybersecurity threats across the nation, the federal government's use of cybersecurity products manufactured by a firm with potential ties to the Russian government is concerning to Congress. In May, the Senate Intelligence Committee held an open hearing where several top U.S. intelligence officials stated with consensus that they would not be comfortable using Kaspersky Lab's products on their systems.[8] Additionally, on June 15, 2017, the House Science Committee Subcommittees on Oversight and Research and Technology held a joint hearing where cybersecurity experts testified on industry approaches and

---

[3] Carol Matlack, *The Company Securing Your Internet Has Close Ties to Russian Spies*, BLOOMBERG BUSINESSWEEK, Mar. 19, 2015, *available at* https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies (last visited June 19, 2017).

[4] Joseph Menn, *Exclusive: Russian Antivirus Firm Faked Malware to Harm Rivals*, REUTERS, Aug. 14, 2015, *available at* www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QJ1CR20150814 (last visited June 27, 2017); *see also* Joseph Menn, *Exclusive: Russia's Kaspersky Threatened to 'Rub Out' Rival, Email Shows*, REUTERS, Aug. 28, 2015, *available at* http://www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QX2GO20150828 (last visited June 27, 2017).

[5] *Id.*

[6] *See* Ali Watkins, *US Officials Are Warning About A Russian Cybersecurity Company's US Government Ties*, BUZZFEED NEWS, May 8, 2017, *available at* https://www.buzzfeed.com/alimwatkins/us-officials-are-warning-about-a-russian-cybersecurity?utm_term=.osyYrP2Mz6#.kexPnOw1Lk (last visited June 19, 2017); *see also* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).

[7] Ken Dilanian & Tom Winter, *Bill Would Bar Pentagon From Business With Russian Cyber Firm Kaspersky*, NBC NEWS, June 28, 2017, *available at* http://www.nbcnews.com/news/us-news/fbi-interviews-employees-russia-linked-cyber-security-firm-kaspersky-lab-n777571 (last visited June 29, 2017); *see also* Joe Uchill, *FBI Visits Kaspersky Lab Employees*, THE HILL, June 28, 2017, *available at* http://thehill.com/policy/cybersecurity/339887-fbi-visits-kaspersky-lab-employees (last visited June 29, 2017).

[8] S. Comm. on Intel., *Worldwide Threats Hearing*, 115th Cong. (May 11, 2017). (question and answer by Senator Marco Rubio).

best practices for safeguarding against future cyber threats.[9] Among the panel of expert witnesses was Salim Neino, CEO of Kryptos Logic—the cybersecurity firm whose employee helped thwart further propagation of the recent WannaCry ransomware attack.[10] In response to questions about the ability of a software manufacturer to embed a "backdoor" into anti-virus software—to facilitate a State's cyber-espionage activities—Mr. Neino alarmingly affirmed that he had "seen that a multitude of times" in the past, and that the barriers to engaging in such activities are "very low."[11] This revelation gives the Committee great concern, especially in light of the capabilities that anti-virus software possesses. Additionally, in response to a question regarding Kaspersky Lab, retired Army General Gregory Touhill, the first federal chief information security officer or CISO, told the Committee: "I buy American."[12]

Anti-virus software is extremely powerful and operates by scanning files at the system level, rather than on the network periphery.[13] As such, other security systems generally do not monitor the operations carried out by the anti-virus software.[14] From a practical perspective, this means that compromised anti-virus software could be used for malicious or nefarious purposes, and could do so without detection. If anti-virus technology or systems are compromised by a user's adversary, it could install malicious code disguised as a security update; it could forego specific updates to pave the way for use of certain vectors of attack; it could forego beneficial updates for a specified subset of users; and it could even extract data that a user's adversary considers valuable.[15] Furthermore, anti-virus is so powerful that it has nearly unimpeded access into all attachments, files, and information contained on a system.[16] In sum, compromised anti-virus has the potential to undermine the security and integrity of any system on which it is installed.

The security and integrity of federal information systems are only as strong as the products that guard them. Although Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, requires federal departments and agencies to implement the NIST Cybersecurity Framework and to provide reports related thereto,[17] the

---

[9] H. Comm. on Science, Space, & Tech. Subcomm. on Research & Tech. jointly with the Subcomm. on Oversight, *Hearing on Bolstering the Government's Cybersecurity: Lessons Learned from WannaCry*, Preliminary Hearing Transcript, 115th Cong. (June 15, 2017) at 61.
[10] *Id.*
[11] *Id.* at 62 (question and answer by Representative Clay Higgins).
[12] *Id.* at 63.
[13] *See* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] The White House, *Executive Order – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017), *available at* https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal (last visited June 29, 2017).

security of federal systems may nevertheless be undermined by compromised anti-virus products. Government contracting data indicating that several federal departments and agencies use or have used cybersecurity or anti-virus products manufactured by Kaspersky Lab is even more troubling.[18] If federal agencies and departments are being guarded by potentially compromised software, then it is virtually impossible for such agencies to effectively and efficiently implement the NIST Framework, and to fully comply with President Trump's executive order. The recent news that Kaspersky Lab's products have been removed from the General Service Administration's contracting Schedule 67 and 70 is encouraging, however federal agencies and contractors may be likely to continue use of Kaspersky Lab's products.[19]

Cybersecurity is a greater threat to our nation than ever before. If these widely reported allegations prove true, then the American public has ample grounds on which to rest their concerns about the security of data stored and transmitted on federal information systems—especially those allegedly protected by Kaspersky Lab's products. In light of this increasing threat, the Committee takes seriously its duty to ensure the NIST Cybersecurity Framework is properly equipped and adapted to safeguard our nation's information. To assist the Committee in understanding the effectiveness of the NIST Framework, and potential vulnerabilities that exist on federal information systems, please provide the following documents and information as soon as possible, but no later than August 11, 2017. Please provide the requested materials for the time frame from January 1, 2013, to present:

1. All documents and communications referring or relating to cybersecurity and/or anti-virus products manufactured by Kaspersky Lab.

2. All documents and communications referring or relating to any evaluation, risk assessment, and decision-making processes on the matter of whether to implement products manufactured by Kaspersky Lab.

3. All documents and communications referring or relating to the use or implementation of products manufactured by Kaspersky Lab.

---

[18] Government Contracting Dataset, *available at* https://www.usaspending.gov/Pages/AdvancedSearch.aspx?k=kaspersky (last visited June 29, 2017); *see* David Goldstein & Greg Gordon, *Exclusive: Kremlin Documents Suggest Link Between Cyber Giant and Russia Spy Agency*, MCCLATCHY, July 3, 2017, *available at* http://www.mcclatchydc.com/news/nation-world/national/article159342694.html (last visited July 12, 2017); *see also* Mike Levine & Pierre Thomas, *Officials Fear Russia Could Try To Target US Through Popular Software Firm Under FBI Scrutiny*, ABC NEWS, May 9, 2017, *available at* http://abcnews.go.com/US/officials-fear-russia-target-us-popular-software-firm/story?id=47295729 (last visited July 12, 2017).

[19] *See* Sarah Kuranda, *Kaspersky Lab Removed From GSA Schedule, Limiting Federal Sales for Its Security Software*, CRN, July 12, 2017, *available at* http://www.crn.com/news/security/300088591/kaspersky-removed-from-gsa-schedule-limiting-federal-sales-for-its-security-software.htm; *see also* Eric Geller, *Trump Administration Restricts Popular Russian Security Software*, POLITICO, July 11, 2017, *available at* http://www.politico.com/story/2017/07/11/trump-russian-security-software-240423.

4. A complete list of any computers, systems, data, media, and/or information utilizing or accessible to Kaspersky Lab products or services.

5. Identify any federal government contractors or subcontractors known to be utilizing Kaspersky Lab's products to fulfill requirements of contracts with the Department or Agency.

6. All documents and communications referring or relating to the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity.

7. All documents and communications referring or relating to the production of reports required by Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.

Pursuant to House Rule X, the Committee on Science, Space, and Technology has jurisdiction over National Institute of Standards and Technology which develops cybersecurity standards and guidelines for the federal government and recommendations for the private sector.

When producing documents to the Committee, please deliver production sets to the Majority Staff in Room 2321 of the Rayburn House Office Building and the Minority Staff in Room 394 of the Ford House Office Building. The Committee prefers, if possible, to receive all documents in electronic format.

If you have any questions about this request, please contact Drew Colliatie or Tom Connally at 202-225-6371. Thank you for your attention to this matter.

Sincerely,

Lamar Smith
Chairman

cc: The Honorable Eddie Bernice Johnson, Ranking Minority Member

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6301
(202) 225–6371
www.science.house.gov

July 27, 2017

The Honorable Robert M. Lightfoot, Jr.
Acting Administrator
National Aeronautics and Space Administration
300 E Street SW
Washington, D.C. 20546

Dear Acting Administrator Lightfoot,

As part of an ongoing review of the federal government's cybersecurity policies and standards, the Committee on Science, Space, and Technology is requesting information and documents from the Administration regarding Kaspersky Lab. The Committee is charged with oversight of the National Institute of Standards and Technology (NIST), and continuously evaluates whether changes to the Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework) are necessary. The documents and information will assist the Committee in determining whether the Framework requires further refinement when implemented by federal departments and agencies.

Kaspersky Lab is among the world's largest cybersecurity companies. Headquartered in Moscow, Russia, it services approximately 400 million users worldwide, including a number of United States Government Agencies and entities.[1] Kaspersky Lab specializes in anti-virus software—products with potentially uninhibited access to the systems they protect.[2] Although Kaspersky Lab was once considered a reputable cybersecurity firm, several concerns have been raised regarding the company and Eugene Kaspersky—the founder and CEO of Kaspersky Lab—and his potential ties to the Russian government.

The Committee is concerned that Kaspersky Lab is susceptible to manipulation by the Russian government, and that its products could be used as a tool for espionage, sabotage, or other nefarious activities against the United States. As early as 2015, reports began to surface

---

[1] *See* Jordan Robertson, *A Russian Cybersecurity Company's Ties to the Kremlin*, BLOOMBERG GOVERNMENT, Jul. 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSXAKB6JIJVL (last visited July 11, 2017).
[2] *See* Jordan Robertson & Michael Riley, *Kaspersky Lab Has Been Working With Russian Intelligence*, BLOOMBERG GOVERNMENT, July 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSX50G6KLVR5 (last visited July 11, 2017).

alleging that Mr. Kaspersky may have "close ties to Russian spies."[3] Shortly thereafter, *Reuters* reported that Kaspersky Lab engaged in a "sabotage" campaign undoubtedly targeting the U.S. cybersecurity market.[4] Specifically, the company "tried to damage rivals in the marketplace by tricking their antivirus software programs into classifying benign files as malicious."[5] More recently, Russia's alleged interference in the 2016 presidential election has heightened public concerns about the Kremlin's desire to meddle with American democratic processes. This, in turn, has ignited speculation over America's cybersecurity posture, and the potential ties that Kaspersky Lab has with the Kremlin. Namely, that the Russian government could use products manufactured by Kaspersky Lab as a medium for engaging in nefarious cyber campaigns against U.S. information systems—including those at several federal departments and agencies—that are purportedly protected by the company's products.[6] Adding to concern, the FBI sent agents to visit "at least a dozen employees of Kaspersky" in order to question them "about the company's operations as part of a counter-intelligence inquiry."[7]

Given the increasing prevalence of cybersecurity threats across the nation, the federal government's use of cybersecurity products manufactured by a firm with potential ties to the Russian government is concerning to Congress. In May, the Senate Intelligence Committee held an open hearing where several top U.S. intelligence officials stated with consensus that they would not be comfortable using Kaspersky Lab's products on their systems.[8] Additionally, on June 15, 2017, the House Science Committee Subcommittees on Oversight and Research and Technology held a joint hearing where cybersecurity experts testified on industry approaches and

---

[3] Carol Matlack, *The Company Securing Your Internet Has Close Ties to Russian Spies*, BLOOMBERG BUSINESSWEEK, Mar. 19, 2015, *available at* https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies (last visited June 19, 2017).

[4] Joseph Menn, *Exclusive: Russian Antivirus Firm Faked Malware to Harm Rivals*, REUTERS, Aug. 14, 2015, *available at* www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QJ1CR20150814 (last visited June 27, 2017); *see also* Joseph Menn, *Exclusive: Russia's Kaspersky Threatened to 'Rub Out' Rival, Email Shows*, REUTERS, Aug. 28, 2015, *available at* http://www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QX2GO20150828 (last visited June 27, 2017).

[5] *Id.*

[6] *See* Ali Watkins, *US Officials Are Warning About A Russian Cybersecurity Company's US Government Ties*, BUZZFEED NEWS, May 8, 2017, *available at* https://www.buzzfeed.com/alimwatkins/us-officials-are-warning-about-a-russian-cybersecurity?utm_term=.osyYrP2Mz6#.kexPnOw1Lk (last visited June 19, 2017); *see also* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).

[7] Ken Dilanian & Tom Winter, *Bill Would Bar Pentagon From Business With Russian Cyber Firm Kaspersky*, NBC NEWS, June 28, 2017, *available at* http://www.nbcnews.com/news/us-news/fbi-interviews-employees-russia-linked-cyber-security-firm-kaspersky-lab-n777571 (last visited June 29, 2017); *see also* Joe Uchill, *FBI Visits Kaspersky Lab Employees*, THE HILL, June 28, 2017, *available at* http://thehill.com/policy/cybersecurity/339887-fbi-visits-kaspersky-lab-employees (last visited June 29, 2017).

[8] S. Comm. on Intel., *Worldwide Threats Hearing*, 115th Cong. (May 11, 2017). (question and answer by Senator Marco Rubio).

best practices for safeguarding against future cyber threats.[9] Among the panel of expert witnesses was Salim Neino, CEO of Kryptos Logic—the cybersecurity firm whose employee helped thwart further propagation of the recent WannaCry ransomware attack.[10] In response to questions about the ability of a software manufacturer to embed a "backdoor" into anti-virus software—to facilitate a State's cyber-espionage activities—Mr. Neino alarmingly affirmed that he had "seen that a multitude of times" in the past, and that the barriers to engaging in such activities are "very low."[11] This revelation gives the Committee great concern, especially in light of the capabilities that anti-virus software possesses. Additionally, in response to a question regarding Kaspersky Lab, retired Army General Gregory Touhill, the first federal chief information security officer or CISO, told the Committee: "I buy American."[12]

Anti-virus software is extremely powerful and operates by scanning files at the system level, rather than on the network periphery.[13] As such, other security systems generally do not monitor the operations carried out by the anti-virus software.[14] From a practical perspective, this means that compromised anti-virus software could be used for malicious or nefarious purposes, and could do so without detection. If anti-virus technology or systems are compromised by a user's adversary, it could install malicious code disguised as a security update; it could forego specific updates to pave the way for use of certain vectors of attack; it could forego beneficial updates for a specified subset of users; and it could even extract data that a user's adversary considers valuable.[15] Furthermore, anti-virus is so powerful that it has nearly unimpeded access into all attachments, files, and information contained on a system.[16] In sum, compromised anti-virus has the potential to undermine the security and integrity of any system on which it is installed.

The security and integrity of federal information systems are only as strong as the products that guard them. Although Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, requires federal departments and agencies to implement the NIST Cybersecurity Framework and to provide reports related thereto,[17] the

---

[9] H. Comm. on Science, Space, & Tech. Subcomm. on Research & Tech. jointly with the Subcomm. on Oversight, *Hearing on Bolstering the Government's Cybersecurity: Lessons Learned from WannaCry*, Preliminary Hearing Transcript, 115th Cong. (June 15, 2017) at 61.
[10] *Id.*
[11] *Id.* at 62 (question and answer by Representative Clay Higgins).
[12] *Id.* at 63.
[13] *See* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] The White House, *Executive Order – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017), *available at* https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal (last visited June 29, 2017).

security of federal systems may nevertheless be undermined by compromised anti-virus products. Government contracting data indicating that several federal departments and agencies use or have used cybersecurity or anti-virus products manufactured by Kaspersky Lab is even more troubling.[18] If federal agencies and departments are being guarded by potentially compromised software, then it is virtually impossible for such agencies to effectively and efficiently implement the NIST Framework, and to fully comply with President Trump's executive order. The recent news that Kaspersky Lab's products have been removed from the General Service Administration's contracting Schedule 67 and 70 is encouraging, however federal agencies and contractors may be likely to continue use of Kaspersky Lab's products.[19]

Cybersecurity is a greater threat to our nation than ever before. If these widely reported allegations prove true, then the American public has ample grounds on which to rest their concerns about the security of data stored and transmitted on federal information systems—especially those allegedly protected by Kaspersky Lab's products. In light of this increasing threat, the Committee takes seriously its duty to ensure the NIST Cybersecurity Framework is properly equipped and adapted to safeguard our nation's information. To assist the Committee in understanding the effectiveness of the NIST Framework, and potential vulnerabilities that exist on federal information systems, please provide the following documents and information as soon as possible, but no later than August 11, 2017. Please provide the requested materials for the time frame from January 1, 2013, to present:

1. All documents and communications referring or relating to cybersecurity and/or anti-virus products manufactured by Kaspersky Lab.

2. All documents and communications referring or relating to any evaluation, risk assessment, and decision-making processes on the matter of whether to implement products manufactured by Kaspersky Lab.

3. All documents and communications referring or relating to the use or implementation of products manufactured by Kaspersky Lab.

---

[18] Government Contracting Dataset, *available at* https://www.usaspending.gov/Pages/AdvancedSearch.aspx?k=kaspersky (last visited June 29, 2017); *see* David Goldstein & Greg Gordon, *Exclusive: Kremlin Documents Suggest Link Between Cyber Giant and Russia Spy Agency*, MCCLATCHY, July 3, 2017, *available at* http://www.mcclatchydc.com/news/nation-world/national/article159342694.html (last visited July 12, 2017); *see also* Mike Levine & Pierre Thomas, *Officials Fear Russia Could Try To Target US Through Popular Software Firm Under FBI Scrutiny*, ABC NEWS, May 9, 2017, *available at* http://abcnews.go.com/US/officials-fear-russia-target-us-popular-software-firm/story?id=47295729 (last visited July 12, 2017).

[19] *See* Sarah Kuranda, *Kaspersky Lab Removed From GSA Schedule, Limiting Federal Sales for Its Security Software*, CRN, July 12, 2017, *available at* http://www.crn.com/news/security/300088591/kaspersky-removed-from-gsa-schedule-limiting-federal-sales-for-its-security-software.htm; *see also* Eric Geller, *Trump Administration Restricts Popular Russian Security Software*, POLITICO, July 11, 2017, *available at* http://www.politico.com/story/2017/07/11/trump-russian-security-software-240423.

4. A complete list of any computers, systems, data, media, and/or information utilizing or accessible to Kaspersky Lab products or services.

5. Identify any federal government contractors or subcontractors known to be utilizing Kaspersky Lab's products to fulfill requirements of contracts with the Department or Agency.

6. All documents and communications referring or relating to the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity.

7. All documents and communications referring or relating to the production of reports required by Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.

Pursuant to House Rule X, the Committee on Science, Space, and Technology has jurisdiction over National Institute of Standards and Technology which develops cybersecurity standards and guidelines for the federal government and recommendations for the private sector.

When producing documents to the Committee, please deliver production sets to the Majority Staff in Room 2321 of the Rayburn House Office Building and the Minority Staff in Room 394 of the Ford House Office Building. The Committee prefers, if possible, to receive all documents in electronic format.

If you have any questions about this request, please contact Drew Colliatie or Tom Connally at 202-225-6371. Thank you for your attention to this matter.

Sincerely,

Lamar Smith
Chairman

cc: The Honorable Eddie Bernice Johnson, Ranking Minority Member

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6301
(202) 225–6371
www.science.house.gov

July 27, 2017

The Honorable Sean Stackley
Acting Secretary
U.S. Department of Navy
1200 Navy Pentagon
Washington D.C. 20350 - 1200

Dear Acting Secretary Stackley,

As part of an ongoing review of the federal government's cybersecurity policies and standards, the Committee on Science, Space, and Technology is requesting information and documents from the Department regarding Kaspersky Lab. The Committee is charged with oversight of the National Institute of Standards and Technology (NIST), and continuously evaluates whether changes to the Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework) are necessary. The documents and information will assist the Committee in determining whether the Framework requires further refinement when implemented by federal departments and agencies.

Kaspersky Lab is among the world's largest cybersecurity companies. Headquartered in Moscow, Russia, it services approximately 400 million users worldwide, including a number of United States Government Agencies and entities.[1] Kaspersky Lab specializes in anti-virus software—products with potentially uninhibited access to the systems they protect.[2] Although Kaspersky Lab was once considered a reputable cybersecurity firm, several concerns have been raised regarding the company and Eugene Kaspersky—the founder and CEO of Kaspersky Lab—and his potential ties to the Russian government.

The Committee is concerned that Kaspersky Lab is susceptible to manipulation by the Russian government, and that its products could be used as a tool for espionage, sabotage, or other nefarious activities against the United States. As early as 2015, reports began to surface

---

[1] *See* Jordan Robertson, *A Russian Cybersecurity Company's Ties to the Kremlin*, BLOOMBERG GOVERNMENT, Jul. 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSXAKB6JIJVL (last visited July 11, 2017).
[2] *See* Jordan Robertson & Michael Riley, *Kaspersky Lab Has Been Working With Russian Intelligence*, BLOOMBERG GOVERNMENT, July 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSX50G6KLVR5 (last visited July 11, 2017).

alleging that Mr. Kaspersky may have "close ties to Russian spies."[3] Shortly thereafter, *Reuters* reported that Kaspersky Lab engaged in a "sabotage" campaign undoubtedly targeting the U.S. cybersecurity market.[4] Specifically, the company "tried to damage rivals in the marketplace by tricking their antivirus software programs into classifying benign files as malicious."[5] More recently, Russia's alleged interference in the 2016 presidential election has heightened public concerns about the Kremlin's desire to meddle with American democratic processes. This, in turn, has ignited speculation over America's cybersecurity posture, and the potential ties that Kaspersky Lab has with the Kremlin. Namely, that the Russian government could use products manufactured by Kaspersky Lab as a medium for engaging in nefarious cyber campaigns against U.S. information systems—including those at several federal departments and agencies—that are purportedly protected by the company's products.[6] Adding to concern, the FBI sent agents to visit "at least a dozen employees of Kaspersky" in order to question them "about the company's operations as part of a counter-intelligence inquiry."[7]

Given the increasing prevalence of cybersecurity threats across the nation, the federal government's use of cybersecurity products manufactured by a firm with potential ties to the Russian government is concerning to Congress. In May, the Senate Intelligence Committee held an open hearing where several top U.S. intelligence officials stated with consensus that they would not be comfortable using Kaspersky Lab's products on their systems.[8] Additionally, on June 15, 2017, the House Science Committee Subcommittees on Oversight and Research and Technology held a joint hearing where cybersecurity experts testified on industry approaches and

---

[3] Carol Matlack, *The Company Securing Your Internet Has Close Ties to Russian Spies*, BLOOMBERG BUSINESSWEEK, Mar. 19, 2015, *available at* https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies (last visited June 19, 2017).

[4] Joseph Menn, *Exclusive: Russian Antivirus Firm Faked Malware to Harm Rivals*, REUTERS, Aug. 14, 2015, *available at* www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QJ1CR20150814 (last visited June 27, 2017); *see also* Joseph Menn, *Exclusive: Russia's Kaspersky Threatened to 'Rub Out' Rival, Email Shows*, REUTERS, Aug. 28, 2015, *available at* http://www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QX2GO20150828 (last visited June 27, 2017).

[5] *Id.*

[6] *See* Ali Watkins, *US Officials Are Warning About A Russian Cybersecurity Company's US Government Ties*, BUZZFEED NEWS, May 8, 2017, *available at* https://www.buzzfeed.com/alimwatkins/us-officials-are-warning-about-a-russian-cybersecurity?utm_term=.osyYrP2Mz6#.kexPnOw1Lk (last visited June 19, 2017); *see also* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).

[7] Ken Dilanian & Tom Winter, *Bill Would Bar Pentagon From Business With Russian Cyber Firm Kaspersky*, NBC NEWS, June 28, 2017, *available at* http://www.nbcnews.com/news/us-news/fbi-interviews-employees-russia-linked-cyber-security-firm-kaspersky-lab-n777571 (last visited June 29, 2017); *see also* Joe Uchill, *FBI Visits Kaspersky Lab Employees*, THE HILL, June 28, 2017, *available at* http://thehill.com/policy/cybersecurity/339887-fbi-visits-kaspersky-lab-employees (last visited June 29, 2017).

[8] S. Comm. on Intel., *Worldwide Threats Hearing*, 115th Cong. (May 11, 2017). (question and answer by Senator Marco Rubio).

best practices for safeguarding against future cyber threats.[9] Among the panel of expert witnesses was Salim Neino, CEO of Kryptos Logic—the cybersecurity firm whose employee helped thwart further propagation of the recent WannaCry ransomware attack.[10] In response to questions about the ability of a software manufacturer to embed a "backdoor" into anti-virus software—to facilitate a State's cyber-espionage activities—Mr. Neino alarmingly affirmed that he had "seen that a multitude of times" in the past, and that the barriers to engaging in such activities are "very low."[11] This revelation gives the Committee great concern, especially in light of the capabilities that anti-virus software possesses. Additionally, in response to a question regarding Kaspersky Lab, retired Army General Gregory Touhill, the first federal chief information security officer or CISO, told the Committee: "I buy American."[12]

Anti-virus software is extremely powerful and operates by scanning files at the system level, rather than on the network periphery.[13] As such, other security systems generally do not monitor the operations carried out by the anti-virus software.[14] From a practical perspective, this means that compromised anti-virus software could be used for malicious or nefarious purposes, and could do so without detection. If anti-virus technology or systems are compromised by a user's adversary, it could install malicious code disguised as a security update; it could forego specific updates to pave the way for use of certain vectors of attack; it could forego beneficial updates for a specified subset of users; and it could even extract data that a user's adversary considers valuable.[15] Furthermore, anti-virus is so powerful that it has nearly unimpeded access into all attachments, files, and information contained on a system.[16] In sum, compromised anti-virus has the potential to undermine the security and integrity of any system on which it is installed.

The security and integrity of federal information systems are only as strong as the products that guard them. Although Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, requires federal departments and agencies to implement the NIST Cybersecurity Framework and to provide reports related thereto,[17] the

---

[9] H. Comm. on Science, Space, & Tech. Subcomm. on Research & Tech. jointly with the Subcomm. on Oversight, *Hearing on Bolstering the Government's Cybersecurity: Lessons Learned from WannaCry*, Preliminary Hearing Transcript, 115th Cong. (June 15, 2017) at 61.
[10] *Id.*
[11] *Id.* at 62 (question and answer by Representative Clay Higgins).
[12] *Id.* at 63.
[13] *See* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] The White House, *Executive Order – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017), *available at* https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal (last visited June 29, 2017).

security of federal systems may nevertheless be undermined by compromised anti-virus products. Government contracting data indicating that several federal departments and agencies use or have used cybersecurity or anti-virus products manufactured by Kaspersky Lab is even more troubling.[18] If federal agencies and departments are being guarded by potentially compromised software, then it is virtually impossible for such agencies to effectively and efficiently implement the NIST Framework, and to fully comply with President Trump's executive order. The recent news that Kaspersky Lab's products have been removed from the General Service Administration's contracting Schedule 67 and 70 is encouraging, however federal agencies and contractors may be likely to continue use of Kaspersky Lab's products.[19]

Cybersecurity is a greater threat to our nation than ever before. If these widely reported allegations prove true, then the American public has ample grounds on which to rest their concerns about the security of data stored and transmitted on federal information systems—especially those allegedly protected by Kaspersky Lab's products. In light of this increasing threat, the Committee takes seriously its duty to ensure the NIST Cybersecurity Framework is properly equipped and adapted to safeguard our nation's information. To assist the Committee in understanding the effectiveness of the NIST Framework, and potential vulnerabilities that exist on federal information systems, please provide the following documents and information as soon as possible, but no later than August 11, 2017. Please provide the requested materials for the time frame from January 1, 2013, to present:

1. All documents and communications referring or relating to cybersecurity and/or anti-virus products manufactured by Kaspersky Lab.

2. All documents and communications referring or relating to any evaluation, risk assessment, and decision-making processes on the matter of whether to implement products manufactured by Kaspersky Lab.

3. All documents and communications referring or relating to the use or implementation of products manufactured by Kaspersky Lab.

---

[18] Government Contracting Dataset, *available at* https://www.usaspending.gov/Pages/AdvancedSearch.aspx?k=kaspersky (last visited June 29, 2017); *see* David Goldstein & Greg Gordon, *Exclusive: Kremlin Documents Suggest Link Between Cyber Giant and Russia Spy Agency*, MCCLATCHY, July 3, 2017, *available at* http://www.mcclatchydc.com/news/nation-world/national/article159342694.html (last visited July 12, 2017); *see also* Mike Levine & Pierre Thomas, *Officials Fear Russia Could Try To Target US Through Popular Software Firm Under FBI Scrutiny*, ABC NEWS, May 9, 2017, *available at* http://abcnews.go.com/US/officials-fear-russia-target-us-popular-software-firm/story?id=47295729 (last visited July 12, 2017).

[19] *See* Sarah Kuranda, *Kaspersky Lab Removed From GSA Schedule, Limiting Federal Sales for Its Security Software*, CRN, July 12, 2017, *available at* http://www.crn.com/news/security/300088591/kaspersky-removed-from-gsa-schedule-limiting-federal-sales-for-its-security-software.htm; *see also* Eric Geller, *Trump Administration Restricts Popular Russian Security Software*, POLITICO, July 11, 2017, *available at* http://www.politico.com/story/2017/07/11/trump-russian-security-software-240423.

4. A complete list of any computers, systems, data, media, and/or information utilizing or accessible to Kaspersky Lab products or services.

5. Identify any federal government contractors or subcontractors known to be utilizing Kaspersky Lab's products to fulfill requirements of contracts with the Department or Agency.

6. All documents and communications referring or relating to the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity.

7. All documents and communications referring or relating to the production of reports required by Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.

Pursuant to House Rule X, the Committee on Science, Space, and Technology has jurisdiction over National Institute of Standards and Technology which develops cybersecurity standards and guidelines for the federal government and recommendations for the private sector.

When producing documents to the Committee, please deliver production sets to the Majority Staff in Room 2321 of the Rayburn House Office Building and the Minority Staff in Room 394 of the Ford House Office Building. The Committee prefers, if possible, to receive all documents in electronic format.

If you have any questions about this request, please contact Drew Colliatie or Tom Connally at 202-225-6371. Thank you for your attention to this matter.

Sincerely,

Lamar Smith
Chairman

cc: The Honorable Eddie Bernice Johnson, Ranking Minority Member

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6301
(202) 225–6371
www.science.house.gov

July 27, 2017

The Honorable Linda McMahon
Administrator
U.S. Small Business Administration
409 3rd Street SW
Washington D.C. 20416

Dear Administrator McMahon,

As part of an ongoing review of the federal government's cybersecurity policies and standards, the Committee on Science, Space, and Technology is requesting information and documents from the Administration regarding Kaspersky Lab. The Committee is charged with oversight of the National Institute of Standards and Technology (NIST), and continuously evaluates whether changes to the Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework) are necessary. The documents and information will assist the Committee in determining whether the Framework requires further refinement when implemented by federal departments and agencies.

Kaspersky Lab is among the world's largest cybersecurity companies. Headquartered in Moscow, Russia, it services approximately 400 million users worldwide, including a number of United States Government Agencies and entities.[1] Kaspersky Lab specializes in anti-virus software—products with potentially uninhibited access to the systems they protect.[2] Although Kaspersky Lab was once considered a reputable cybersecurity firm, several concerns have been raised regarding the company and Eugene Kaspersky—the founder and CEO of Kaspersky Lab—and his potential ties to the Russian government.

The Committee is concerned that Kaspersky Lab is susceptible to manipulation by the Russian government, and that its products could be used as a tool for espionage, sabotage, or other nefarious activities against the United States. As early as 2015, reports began to surface

---

[1] *See* Jordan Robertson, *A Russian Cybersecurity Company's Ties to the Kremlin*, BLOOMBERG GOVERNMENT, Jul. 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSXAKB6JIJVL (last visited July 11, 2017).
[2] *See* Jordan Robertson & Michael Riley, *Kaspersky Lab Has Been Working With Russian Intelligence*, BLOOMBERG GOVERNMENT, July 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSX50G6KLVR5 (last visited July 11, 2017).

alleging that Mr. Kaspersky may have "close ties to Russian spies."[3] Shortly thereafter, *Reuters* reported that Kaspersky Lab engaged in a "sabotage" campaign undoubtedly targeting the U.S. cybersecurity market.[4] Specifically, the company "tried to damage rivals in the marketplace by tricking their antivirus software programs into classifying benign files as malicious."[5] More recently, Russia's alleged interference in the 2016 presidential election has heightened public concerns about the Kremlin's desire to meddle with American democratic processes. This, in turn, has ignited speculation over America's cybersecurity posture, and the potential ties that Kaspersky Lab has with the Kremlin. Namely, that the Russian government could use products manufactured by Kaspersky Lab as a medium for engaging in nefarious cyber campaigns against U.S. information systems—including those at several federal departments and agencies—that are purportedly protected by the company's products.[6] Adding to concern, the FBI sent agents to visit "at least a dozen employees of Kaspersky" in order to question them "about the company's operations as part of a counter-intelligence inquiry."[7]

Given the increasing prevalence of cybersecurity threats across the nation, the federal government's use of cybersecurity products manufactured by a firm with potential ties to the Russian government is concerning to Congress. In May, the Senate Intelligence Committee held an open hearing where several top U.S. intelligence officials stated with consensus that they would not be comfortable using Kaspersky Lab's products on their systems.[8] Additionally, on June 15, 2017, the House Science Committee Subcommittees on Oversight and Research and Technology held a joint hearing where cybersecurity experts testified on industry approaches and

---

[3] Carol Matlack, *The Company Securing Your Internet Has Close Ties to Russian Spies*, BLOOMBERG BUSINESSWEEK, Mar. 19, 2015, *available at* https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies (last visited June 19, 2017).

[4] Joseph Menn, *Exclusive: Russian Antivirus Firm Faked Malware to Harm Rivals*, REUTERS, Aug. 14, 2015, *available at* www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QJ1CR20150814 (last visited June 27, 2017); *see also* Joseph Menn, *Exclusive: Russia's Kaspersky Threatened to 'Rub Out' Rival, Email Shows*, REUTERS, Aug. 28, 2015, *available at* http://www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QX2GO20150828 (last visited June 27, 2017).

[5] *Id.*

[6] *See* Ali Watkins, *US Officials Are Warning About A Russian Cybersecurity Company's US Government Ties*, BUZZFEED NEWS, May 8, 2017, *available at* https://www.buzzfeed.com/alimwatkins/us-officials-are-warning-about-a-russian-cybersecurity?utm_term=.osyYrP2Mz6#.kexPnOw1Lk (last visited June 19, 2017); *see also* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).

[7] Ken Dilanian & Tom Winter, *Bill Would Bar Pentagon From Business With Russian Cyber Firm Kaspersky*, NBC NEWS, June 28, 2017, *available at* http://www.nbcnews.com/news/us-news/fbi-interviews-employees-russia-linked-cyber-security-firm-kaspersky-lab-n777571 (last visited June 29, 2017); *see also* Joe Uchill, *FBI Visits Kaspersky Lab Employees*, THE HILL, June 28, 2017, *available at* http://thehill.com/policy/cybersecurity/339887-fbi-visits-kaspersky-lab-employees (last visited June 29, 2017).

[8] S. Comm. on Intel., *Worldwide Threats Hearing*, 115th Cong. (May 11, 2017). (question and answer by Senator Marco Rubio).

best practices for safeguarding against future cyber threats.[9] Among the panel of expert witnesses was Salim Neino, CEO of Kryptos Logic—the cybersecurity firm whose employee helped thwart further propagation of the recent WannaCry ransomware attack.[10] In response to questions about the ability of a software manufacturer to embed a "backdoor" into anti-virus software—to facilitate a State's cyber-espionage activities—Mr. Neino alarmingly affirmed that he had "seen that a multitude of times" in the past, and that the barriers to engaging in such activities are "very low."[11] This revelation gives the Committee great concern, especially in light of the capabilities that anti-virus software possesses. Additionally, in response to a question regarding Kaspersky Lab, retired Army General Gregory Touhill, the first federal chief information security officer or CISO, told the Committee: "I buy American."[12]

Anti-virus software is extremely powerful and operates by scanning files at the system level, rather than on the network periphery.[13] As such, other security systems generally do not monitor the operations carried out by the anti-virus software.[14] From a practical perspective, this means that compromised anti-virus software could be used for malicious or nefarious purposes, and could do so without detection. If anti-virus technology or systems are compromised by a user's adversary, it could install malicious code disguised as a security update; it could forego specific updates to pave the way for use of certain vectors of attack; it could forego beneficial updates for a specified subset of users; and it could even extract data that a user's adversary considers valuable.[15] Furthermore, anti-virus is so powerful that it has nearly unimpeded access into all attachments, files, and information contained on a system.[16] In sum, compromised anti-virus has the potential to undermine the security and integrity of any system on which it is installed.

The security and integrity of federal information systems are only as strong as the products that guard them. Although Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, requires federal departments and agencies to implement the NIST Cybersecurity Framework and to provide reports related thereto,[17] the

---

[9] H. Comm. on Science, Space, & Tech. Subcomm. on Research & Tech. jointly with the Subcomm. on Oversight, *Hearing on Bolstering the Government's Cybersecurity: Lessons Learned from WannaCry*, Preliminary Hearing Transcript, 115th Cong. (June 15, 2017) at 61.
[10] *Id.*
[11] *Id.* at 62 (question and answer by Representative Clay Higgins).
[12] *Id.* at 63.
[13] *See* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] The White House, *Executive Order – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017), *available at* https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal (last visited June 29, 2017).

security of federal systems may nevertheless be undermined by compromised anti-virus products. Government contracting data indicating that several federal departments and agencies use or have used cybersecurity or anti-virus products manufactured by Kaspersky Lab is even more troubling.[18] If federal agencies and departments are being guarded by potentially compromised software, then it is virtually impossible for such agencies to effectively and efficiently implement the NIST Framework, and to fully comply with President Trump's executive order. The recent news that Kaspersky Lab's products have been removed from the General Service Administration's contracting Schedule 67 and 70 is encouraging, however federal agencies and contractors may be likely to continue use of Kaspersky Lab's products.[19]

Cybersecurity is a greater threat to our nation than ever before. If these widely reported allegations prove true, then the American public has ample grounds on which to rest their concerns about the security of data stored and transmitted on federal information systems—especially those allegedly protected by Kaspersky Lab's products. In light of this increasing threat, the Committee takes seriously its duty to ensure the NIST Cybersecurity Framework is properly equipped and adapted to safeguard our nation's information. To assist the Committee in understanding the effectiveness of the NIST Framework, and potential vulnerabilities that exist on federal information systems, please provide the following documents and information as soon as possible, but no later than August 11, 2017. Please provide the requested materials for the time frame from January 1, 2013, to present:

1. All documents and communications referring or relating to cybersecurity and/or anti-virus products manufactured by Kaspersky Lab.

2. All documents and communications referring or relating to any evaluation, risk assessment, and decision-making processes on the matter of whether to implement products manufactured by Kaspersky Lab.

3. All documents and communications referring or relating to the use or implementation of products manufactured by Kaspersky Lab.

---

[18] Government Contracting Dataset, *available at* https://www.usaspending.gov/Pages/AdvancedSearch.aspx?k=kaspersky (last visited June 29, 2017); *see* David Goldstein & Greg Gordon, *Exclusive: Kremlin Documents Suggest Link Between Cyber Giant and Russia Spy Agency*, MCCLATCHY, July 3, 2017, *available at* http://www.mcclatchydc.com/news/nation-world/national/article159342694.html (last visited July 12, 2017); *see also* Mike Levine & Pierre Thomas, *Officials Fear Russia Could Try To Target US Through Popular Software Firm Under FBI Scrutiny*, ABC NEWS, May 9, 2017, *available at* http://abcnews.go.com/US/officials-fear-russia-target-us-popular-software-firm/story?id=47295729 (last visited July 12, 2017).

[19] *See* Sarah Kuranda, *Kaspersky Lab Removed From GSA Schedule, Limiting Federal Sales for Its Security Software*, CRN, July 12, 2017, *available at* http://www.crn.com/news/security/300088591/kaspersky-removed-from-gsa-schedule-limiting-federal-sales-for-its-security-software.htm; *see also* Eric Geller, *Trump Administration Restricts Popular Russian Security Software*, POLITICO, July 11, 2017, *available at* http://www.politico.com/story/2017/07/11/trump-russian-security-software-240423.

4. A complete list of any computers, systems, data, media, and/or information utilizing or accessible to Kaspersky Lab products or services.

5. Identify any federal government contractors or subcontractors known to be utilizing Kaspersky Lab's products to fulfill requirements of contracts with the Department or Agency.

6. All documents and communications referring or relating to the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity.

7. All documents and communications referring or relating to the production of reports required by Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.

Pursuant to House Rule X, the Committee on Science, Space, and Technology has jurisdiction over National Institute of Standards and Technology which develops cybersecurity standards and guidelines for the federal government and recommendations for the private sector.

When producing documents to the Committee, please deliver production sets to the Majority Staff in Room 2321 of the Rayburn House Office Building and the Minority Staff in Room 394 of the Ford House Office Building. The Committee prefers, if possible, to receive all documents in electronic format.

If you have any questions about this request, please contact Drew Colliatie or Tom Connally at 202-225-6371. Thank you for your attention to this matter.

Sincerely,

Lamar Smith

Lamar Smith
Chairman

cc: The Honorable Eddie Bernice Johnson, Ranking Minority Member

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6301
(202) 225–6371
www.science.house.gov

July 27, 2017

The Honorable Rex W. Tillerson
Secretary
U.S. Department of State
2201 C Street NW
Suite 2236
Washington D.C. 20520

Dear Secretary Tillerson,

As part of an ongoing review of the federal government's cybersecurity policies and standards, the Committee on Science, Space, and Technology is requesting information and documents from the Department regarding Kaspersky Lab. The Committee is charged with oversight of the National Institute of Standards and Technology (NIST), and continuously evaluates whether changes to the Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework) are necessary. The documents and information will assist the Committee in determining whether the Framework requires further refinement when implemented by federal departments and agencies.

Kaspersky Lab is among the world's largest cybersecurity companies. Headquartered in Moscow, Russia, it services approximately 400 million users worldwide, including a number of United States Government Agencies and entities.[1] Kaspersky Lab specializes in anti-virus software—products with potentially uninhibited access to the systems they protect.[2] Although Kaspersky Lab was once considered a reputable cybersecurity firm, several concerns have been raised regarding the company and Eugene Kaspersky—the founder and CEO of Kaspersky Lab—and his potential ties to the Russian government.

The Committee is concerned that Kaspersky Lab is susceptible to manipulation by the Russian government, and that its products could be used as a tool for espionage, sabotage, or other nefarious activities against the United States. As early as 2015, reports began to surface

---

[1] *See* Jordan Robertson, *A Russian Cybersecurity Company's Ties to the Kremlin*, BLOOMBERG GOVERNMENT, Jul. 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSXAKB6JIJVL (last visited July 11, 2017).
[2] *See* Jordan Robertson & Michael Riley, *Kaspersky Lab Has Been Working With Russian Intelligence*, BLOOMBERG GOVERNMENT, July 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSX50G6KLVR5 (last visited July 11, 2017).

alleging that Mr. Kaspersky may have "close ties to Russian spies."[3] Shortly thereafter, *Reuters* reported that Kaspersky Lab engaged in a "sabotage" campaign undoubtedly targeting the U.S. cybersecurity market.[4] Specifically, the company "tried to damage rivals in the marketplace by tricking their antivirus software programs into classifying benign files as malicious."[5] More recently, Russia's alleged interference in the 2016 presidential election has heightened public concerns about the Kremlin's desire to meddle with American democratic processes. This, in turn, has ignited speculation over America's cybersecurity posture, and the potential ties that Kaspersky Lab has with the Kremlin. Namely, that the Russian government could use products manufactured by Kaspersky Lab as a medium for engaging in nefarious cyber campaigns against U.S. information systems—including those at several federal departments and agencies—that are purportedly protected by the company's products.[6] Adding to concern, the FBI sent agents to visit "at least a dozen employees of Kaspersky" in order to question them "about the company's operations as part of a counter-intelligence inquiry."[7]

Given the increasing prevalence of cybersecurity threats across the nation, the federal government's use of cybersecurity products manufactured by a firm with potential ties to the Russian government is concerning to Congress. In May, the Senate Intelligence Committee held an open hearing where several top U.S. intelligence officials stated with consensus that they would not be comfortable using Kaspersky Lab's products on their systems.[8] Additionally, on June 15, 2017, the House Science Committee Subcommittees on Oversight and Research and Technology held a joint hearing where cybersecurity experts testified on industry approaches and

---

[3] Carol Matlack, *The Company Securing Your Internet Has Close Ties to Russian Spies*, BLOOMBERG BUSINESSWEEK, Mar. 19, 2015, *available at* https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies (last visited June 19, 2017).

[4] Joseph Menn, *Exclusive: Russian Antivirus Firm Faked Malware to Harm Rivals*, REUTERS, Aug. 14, 2015, *available at* www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QJ1CR20150814 (last visited June 27, 2017); *see also* Joseph Menn, *Exclusive: Russia's Kaspersky Threatened to 'Rub Out' Rival, Email Shows*, REUTERS, Aug. 28, 2015, *available at* http://www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QX2GO20150828 (last visited June 27, 2017).

[5] *Id.*

[6] *See* Ali Watkins, *US Officials Are Warning About A Russian Cybersecurity Company's US Government Ties*, BUZZFEED NEWS, May 8, 2017, *available at* https://www.buzzfeed.com/alimwatkins/us-officials-are-warning-about-a-russian-cybersecurity?utm_term=.osyYrP2Mz6#.kexPnOw1Lk (last visited June 19, 2017); *see also* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).

[7] Ken Dilanian & Tom Winter, *Bill Would Bar Pentagon From Business With Russian Cyber Firm Kaspersky*, NBC NEWS, June 28, 2017, *available at* http://www.nbcnews.com/news/us-news/fbi-interviews-employees-russia-linked-cyber-security-firm-kaspersky-lab-n777571 (last visited June 29, 2017); *see also* Joe Uchill, *FBI Visits Kaspersky Lab Employees*, THE HILL, June 28, 2017, *available at* http://thehill.com/policy/cybersecurity/339887-fbi-visits-kaspersky-lab-employees (last visited June 29, 2017).

[8] S. Comm. on Intel., *Worldwide Threats Hearing*, 115th Cong. (May 11, 2017). (question and answer by Senator Marco Rubio).

best practices for safeguarding against future cyber threats.[9] Among the panel of expert witnesses was Salim Neino, CEO of Kryptos Logic—the cybersecurity firm whose employee helped thwart further propagation of the recent WannaCry ransomware attack.[10] In response to questions about the ability of a software manufacturer to embed a "backdoor" into anti-virus software—to facilitate a State's cyber-espionage activities—Mr. Neino alarmingly affirmed that he had "seen that a multitude of times" in the past, and that the barriers to engaging in such activities are "very low."[11] This revelation gives the Committee great concern, especially in light of the capabilities that anti-virus software possesses. Additionally, in response to a question regarding Kaspersky Lab, retired Army General Gregory Touhill, the first federal chief information security officer or CISO, told the Committee: "I buy American."[12]

Anti-virus software is extremely powerful and operates by scanning files at the system level, rather than on the network periphery.[13] As such, other security systems generally do not monitor the operations carried out by the anti-virus software.[14] From a practical perspective, this means that compromised anti-virus software could be used for malicious or nefarious purposes, and could do so without detection. If anti-virus technology or systems are compromised by a user's adversary, it could install malicious code disguised as a security update; it could forego specific updates to pave the way for use of certain vectors of attack; it could forego beneficial updates for a specified subset of users; and it could even extract data that a user's adversary considers valuable.[15] Furthermore, anti-virus is so powerful that it has nearly unimpeded access into all attachments, files, and information contained on a system.[16] In sum, compromised anti-virus has the potential to undermine the security and integrity of any system on which it is installed.

The security and integrity of federal information systems are only as strong as the products that guard them. Although Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, requires federal departments and agencies to implement the NIST Cybersecurity Framework and to provide reports related thereto,[17] the

---

[9] H. Comm. on Science, Space, & Tech. Subcomm. on Research & Tech. jointly with the Subcomm. on Oversight, *Hearing on Bolstering the Government's Cybersecurity: Lessons Learned from WannaCry*, Preliminary Hearing Transcript, 115th Cong. (June 15, 2017) at 61.
[10] *Id.*
[11] *Id.* at 62 (question and answer by Representative Clay Higgins).
[12] *Id.* at 63.
[13] *See* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] The White House, *Executive Order – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017), *available at* https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal (last visited June 29, 2017).

security of federal systems may nevertheless be undermined by compromised anti-virus products. Government contracting data indicating that several federal departments and agencies use or have used cybersecurity or anti-virus products manufactured by Kaspersky Lab is even more troubling.[18] If federal agencies and departments are being guarded by potentially compromised software, then it is virtually impossible for such agencies to effectively and efficiently implement the NIST Framework, and to fully comply with President Trump's executive order. The recent news that Kaspersky Lab's products have been removed from the General Service Administration's contracting Schedule 67 and 70 is encouraging, however federal agencies and contractors may be likely to continue use of Kaspersky Lab's products.[19]

Cybersecurity is a greater threat to our nation than ever before. If these widely reported allegations prove true, then the American public has ample grounds on which to rest their concerns about the security of data stored and transmitted on federal information systems—especially those allegedly protected by Kaspersky Lab's products. In light of this increasing threat, the Committee takes seriously its duty to ensure the NIST Cybersecurity Framework is properly equipped and adapted to safeguard our nation's information. To assist the Committee in understanding the effectiveness of the NIST Framework, and potential vulnerabilities that exist on federal information systems, please provide the following documents and information as soon as possible, but no later than August 11, 2017. Please provide the requested materials for the time frame from January 1, 2013, to present:

1. All documents and communications referring or relating to cybersecurity and/or anti-virus products manufactured by Kaspersky Lab.

2. All documents and communications referring or relating to any evaluation, risk assessment, and decision-making processes on the matter of whether to implement products manufactured by Kaspersky Lab.

3. All documents and communications referring or relating to the use or implementation of products manufactured by Kaspersky Lab.

---

[18] Government Contracting Dataset, *available at* https://www.usaspending.gov/Pages/AdvancedSearch.aspx?k=kaspersky (last visited June 29, 2017); *see* David Goldstein & Greg Gordon, *Exclusive: Kremlin Documents Suggest Link Between Cyber Giant and Russia Spy Agency*, MCCLATCHY, July 3, 2017, *available at* http://www.mcclatchydc.com/news/nation-world/national/article159342694.html (last visited July 12, 2017); *see also* Mike Levine & Pierre Thomas, *Officials Fear Russia Could Try To Target US Through Popular Software Firm Under FBI Scrutiny*, ABC NEWS, May 9, 2017, *available at* http://abcnews.go.com/US/officials-fear-russia-target-us-popular-software-firm/story?id=47295729 (last visited July 12, 2017).

[19] *See* Sarah Kuranda, *Kaspersky Lab Removed From GSA Schedule, Limiting Federal Sales for Its Security Software*, CRN, July 12, 2017, *available at* http://www.crn.com/news/security/300088591/kaspersky-removed-from-gsa-schedule-limiting-federal-sales-for-its-security-software.htm; *see also* Eric Geller, *Trump Administration Restricts Popular Russian Security Software*, POLITICO, July 11, 2017, *available at* http://www.politico.com/story/2017/07/11/trump-russian-security-software-240423.

4. A complete list of any computers, systems, data, media, and/or information utilizing or accessible to Kaspersky Lab products or services.

5. Identify any federal government contractors or subcontractors known to be utilizing Kaspersky Lab's products to fulfill requirements of contracts with the Department or Agency.

6. All documents and communications referring or relating to the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity.

7. All documents and communications referring or relating to the production of reports required by Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.

Pursuant to House Rule X, the Committee on Science, Space, and Technology has jurisdiction over National Institute of Standards and Technology which develops cybersecurity standards and guidelines for the federal government and recommendations for the private sector.

When producing documents to the Committee, please deliver production sets to the Majority Staff in Room 2321 of the Rayburn House Office Building and the Minority Staff in Room 394 of the Ford House Office Building. The Committee prefers, if possible, to receive all documents in electronic format.

If you have any questions about this request, please contact Drew Colliatie or Tom Connally at 202-225-6371. Thank you for your attention to this matter.

Sincerely,

Lamar Smith
Chairman

cc: The Honorable Eddie Bernice Johnson, Ranking Minority Member

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6301
(202) 225–6371
www.science.house.gov

July 27, 2017

The Honorable Steven Mnuchin
Secretary
U.S. Department of Treasury
1500 Pennsylvania Avenue NW
Washington D.C. 20220

Dear Secretary Mnuchin,

As part of an ongoing review of the federal government's cybersecurity policies and standards, the Committee on Science, Space, and Technology is requesting information and documents from the Department regarding Kaspersky Lab. The Committee is charged with oversight of the National Institute of Standards and Technology (NIST), and continuously evaluates whether changes to the Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework) are necessary. The documents and information will assist the Committee in determining whether the Framework requires further refinement when implemented by federal departments and agencies.

Kaspersky Lab is among the world's largest cybersecurity companies. Headquartered in Moscow, Russia, it services approximately 400 million users worldwide, including a number of United States Government Agencies and entities.[1] Kaspersky Lab specializes in anti-virus software—products with potentially uninhibited access to the systems they protect.[2] Although Kaspersky Lab was once considered a reputable cybersecurity firm, several concerns have been raised regarding the company and Eugene Kaspersky—the founder and CEO of Kaspersky Lab—and his potential ties to the Russian government.

The Committee is concerned that Kaspersky Lab is susceptible to manipulation by the Russian government, and that its products could be used as a tool for espionage, sabotage, or other nefarious activities against the United States. As early as 2015, reports began to surface

---

[1] *See* Jordan Robertson, *A Russian Cybersecurity Company's Ties to the Kremlin*, BLOOMBERG GOVERNMENT, Jul. 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSXAKB6JIJVL (last visited July 11, 2017).
[2] *See* Jordan Robertson & Michael Riley, *Kaspersky Lab Has Been Working With Russian Intelligence*, BLOOMBERG GOVERNMENT, July 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSX50G6KLVR5 (last visited July 11, 2017).

alleging that Mr. Kaspersky may have "close ties to Russian spies."[3] Shortly thereafter, *Reuters* reported that Kaspersky Lab engaged in a "sabotage" campaign undoubtedly targeting the U.S. cybersecurity market.[4] Specifically, the company "tried to damage rivals in the marketplace by tricking their antivirus software programs into classifying benign files as malicious."[5] More recently, Russia's alleged interference in the 2016 presidential election has heightened public concerns about the Kremlin's desire to meddle with American democratic processes. This, in turn, has ignited speculation over America's cybersecurity posture, and the potential ties that Kaspersky Lab has with the Kremlin. Namely, that the Russian government could use products manufactured by Kaspersky Lab as a medium for engaging in nefarious cyber campaigns against U.S. information systems—including those at several federal departments and agencies—that are purportedly protected by the company's products.[6] Adding to concern, the FBI sent agents to visit "at least a dozen employees of Kaspersky" in order to question them "about the company's operations as part of a counter-intelligence inquiry."[7]

Given the increasing prevalence of cybersecurity threats across the nation, the federal government's use of cybersecurity products manufactured by a firm with potential ties to the Russian government is concerning to Congress. In May, the Senate Intelligence Committee held an open hearing where several top U.S. intelligence officials stated with consensus that they would not be comfortable using Kaspersky Lab's products on their systems.[8] Additionally, on June 15, 2017, the House Science Committee Subcommittees on Oversight and Research and Technology held a joint hearing where cybersecurity experts testified on industry approaches and

---

[3] Carol Matlack, *The Company Securing Your Internet Has Close Ties to Russian Spies*, BLOOMBERG BUSINESSWEEK, Mar. 19, 2015, *available at* https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies (last visited June 19, 2017).

[4] Joseph Menn, *Exclusive: Russian Antivirus Firm Faked Malware to Harm Rivals*, REUTERS, Aug. 14, 2015, *available at* www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QJ1CR20150814 (last visited June 27, 2017); *see also* Joseph Menn, *Exclusive: Russia's Kaspersky Threatened to 'Rub Out' Rival, Email Shows*, REUTERS, Aug. 28, 2015, *available at* http://www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QX2GO20150828 (last visited June 27, 2017).

[5] *Id.*

[6] *See* Ali Watkins, *US Officials Are Warning About A Russian Cybersecurity Company's US Government Ties*, BUZZFEED NEWS, May 8, 2017, *available at* https://www.buzzfeed.com/alimwatkins/us-officials-are-warning-about-a-russian-cybersecurity?utm_term=.osyYrP2Mz6#.kexPnOw1Lk (last visited June 19, 2017); *see also* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).

[7] Ken Dilanian & Tom Winter, *Bill Would Bar Pentagon From Business With Russian Cyber Firm Kaspersky*, NBC NEWS, June 28, 2017, *available at* http://www.nbcnews.com/news/us-news/fbi-interviews-employees-russia-linked-cyber-security-firm-kaspersky-lab-n777571 (last visited June 29, 2017); *see also* Joe Uchill, *FBI Visits Kaspersky Lab Employees*, THE HILL, June 28, 2017, *available at* http://thehill.com/policy/cybersecurity/339887-fbi-visits-kaspersky-lab-employees (last visited June 29, 2017).

[8] S. Comm. on Intel., *Worldwide Threats Hearing*, 115th Cong. (May 11, 2017). (question and answer by Senator Marco Rubio).

best practices for safeguarding against future cyber threats.[9] Among the panel of expert witnesses was Salim Neino, CEO of Kryptos Logic—the cybersecurity firm whose employee helped thwart further propagation of the recent WannaCry ransomware attack.[10] In response to questions about the ability of a software manufacturer to embed a "backdoor" into anti-virus software—to facilitate a State's cyber-espionage activities—Mr. Neino alarmingly affirmed that he had "seen that a multitude of times" in the past, and that the barriers to engaging in such activities are "very low."[11] This revelation gives the Committee great concern, especially in light of the capabilities that anti-virus software possesses. Additionally, in response to a question regarding Kaspersky Lab, retired Army General Gregory Touhill, the first federal chief information security officer or CISO, told the Committee: "I buy American."[12]

Anti-virus software is extremely powerful and operates by scanning files at the system level, rather than on the network periphery.[13] As such, other security systems generally do not monitor the operations carried out by the anti-virus software.[14] From a practical perspective, this means that compromised anti-virus software could be used for malicious or nefarious purposes, and could do so without detection. If anti-virus technology or systems are compromised by a user's adversary, it could install malicious code disguised as a security update; it could forego specific updates to pave the way for use of certain vectors of attack; it could forego beneficial updates for a specified subset of users; and it could even extract data that a user's adversary considers valuable.[15] Furthermore, anti-virus is so powerful that it has nearly unimpeded access into all attachments, files, and information contained on a system.[16] In sum, compromised anti-virus has the potential to undermine the security and integrity of any system on which it is installed.

The security and integrity of federal information systems are only as strong as the products that guard them. Although Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, requires federal departments and agencies to implement the NIST Cybersecurity Framework and to provide reports related thereto,[17] the

---

[9] H. Comm. on Science, Space, & Tech. Subcomm. on Research & Tech. jointly with the Subcomm. on Oversight, *Hearing on Bolstering the Government's Cybersecurity: Lessons Learned from WannaCry*, Preliminary Hearing Transcript, 115th Cong. (June 15, 2017) at 61.
[10] *Id.*
[11] *Id.* at 62 (question and answer by Representative Clay Higgins).
[12] *Id.* at 63.
[13] *See* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] The White House, *Executive Order – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017), *available at* https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal (last visited June 29, 2017).

security of federal systems may nevertheless be undermined by compromised anti-virus products. Government contracting data indicating that several federal departments and agencies use or have used cybersecurity or anti-virus products manufactured by Kaspersky Lab is even more troubling.[18] If federal agencies and departments are being guarded by potentially compromised software, then it is virtually impossible for such agencies to effectively and efficiently implement the NIST Framework, and to fully comply with President Trump's executive order. The recent news that Kaspersky Lab's products have been removed from the General Service Administration's contracting Schedule 67 and 70 is encouraging, however federal agencies and contractors may be likely to continue use of Kaspersky Lab's products.[19]

Cybersecurity is a greater threat to our nation than ever before. If these widely reported allegations prove true, then the American public has ample grounds on which to rest their concerns about the security of data stored and transmitted on federal information systems—especially those allegedly protected by Kaspersky Lab's products. In light of this increasing threat, the Committee takes seriously its duty to ensure the NIST Cybersecurity Framework is properly equipped and adapted to safeguard our nation's information. To assist the Committee in understanding the effectiveness of the NIST Framework, and potential vulnerabilities that exist on federal information systems, please provide the following documents and information as soon as possible, but no later than August 11, 2017. Please provide the requested materials for the time frame from January 1, 2013, to present:

1. All documents and communications referring or relating to cybersecurity and/or anti-virus products manufactured by Kaspersky Lab.

2. All documents and communications referring or relating to any evaluation, risk assessment, and decision-making processes on the matter of whether to implement products manufactured by Kaspersky Lab.

3. All documents and communications referring or relating to the use or implementation of products manufactured by Kaspersky Lab.

---

[18] Government Contracting Dataset, *available at* https://www.usaspending.gov/Pages/AdvancedSearch.aspx?k=kaspersky (last visited June 29, 2017); *see* David Goldstein & Greg Gordon, *Exclusive: Kremlin Documents Suggest Link Between Cyber Giant and Russia Spy Agency*, MCCLATCHY, July 3, 2017, *available at* http://www.mcclatchydc.com/news/nation-world/national/article159342694.html (last visited July 12, 2017); *see also* Mike Levine & Pierre Thomas, *Officials Fear Russia Could Try To Target US Through Popular Software Firm Under FBI Scrutiny*, ABC NEWS, May 9, 2017, *available at* http://abcnews.go.com/US/officials-fear-russia-target-us-popular-software-firm/story?id=47295729 (last visited July 12, 2017).

[19] *See* Sarah Kuranda, *Kaspersky Lab Removed From GSA Schedule, Limiting Federal Sales for Its Security Software*, CRN, July 12, 2017, *available at* http://www.crn.com/news/security/300088591/kaspersky-removed-from-gsa-schedule-limiting-federal-sales-for-its-security-software.htm; *see also* Eric Geller, *Trump Administration Restricts Popular Russian Security Software*, POLITICO, July 11, 2017, *available at* http://www.politico.com/story/2017/07/11/trump-russian-security-software-240423.

4. A complete list of any computers, systems, data, media, and/or information utilizing or accessible to Kaspersky Lab products or services.

5. Identify any federal government contractors or subcontractors known to be utilizing Kaspersky Lab's products to fulfill requirements of contracts with the Department or Agency.

6. All documents and communications referring or relating to the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity.

7. All documents and communications referring or relating to the production of reports required by Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.

Pursuant to House Rule X, the Committee on Science, Space, and Technology has jurisdiction over National Institute of Standards and Technology which develops cybersecurity standards and guidelines for the federal government and recommendations for the private sector.

When producing documents to the Committee, please deliver production sets to the Majority Staff in Room 2321 of the Rayburn House Office Building and the Minority Staff in Room 394 of the Ford House Office Building. The Committee prefers, if possible, to receive all documents in electronic format.

If you have any questions about this request, please contact Drew Colliatie or Tom Connally at 202-225-6371. Thank you for your attention to this matter.

Sincerely,

Lamar Smith
Chairman

cc: The Honorable Eddie Bernice Johnson, Ranking Minority Member

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6301
(202) 225–6371
www.science.house.gov

July 27, 2017

The Honorable David Shulkin
Secretary
U.S. Department of Veterans' Affairs
810 Vermont Avenue NW
Washington D.C. 20420

Dear Secretary Shulkin,

As part of an ongoing review of the federal government's cybersecurity policies and standards, the Committee on Science, Space, and Technology is requesting information and documents from the Department regarding Kaspersky Lab. The Committee is charged with oversight of the National Institute of Standards and Technology (NIST), and continuously evaluates whether changes to the Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework) are necessary. The documents and information will assist the Committee in determining whether the Framework requires further refinement when implemented by federal departments and agencies.

Kaspersky Lab is among the world's largest cybersecurity companies. Headquartered in Moscow, Russia, it services approximately 400 million users worldwide, including a number of United States Government Agencies and entities.[1] Kaspersky Lab specializes in anti-virus software—products with potentially uninhibited access to the systems they protect.[2] Although Kaspersky Lab was once considered a reputable cybersecurity firm, several concerns have been raised regarding the company and Eugene Kaspersky—the founder and CEO of Kaspersky Lab—and his potential ties to the Russian government.

The Committee is concerned that Kaspersky Lab is susceptible to manipulation by the Russian government, and that its products could be used as a tool for espionage, sabotage, or other nefarious activities against the United States. As early as 2015, reports began to surface

---

[1] *See* Jordan Robertson, *A Russian Cybersecurity Company's Ties to the Kremlin*, BLOOMBERG GOVERNMENT, Jul. 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSXAKB6JIJVL (last visited July 11, 2017).
[2] *See* Jordan Robertson & Michael Riley, *Kaspersky Lab Has Been Working With Russian Intelligence*, BLOOMBERG GOVERNMENT, July 11, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OSX50G6KLVR5 (last visited July 11, 2017).

alleging that Mr. Kaspersky may have "close ties to Russian spies."[3] Shortly thereafter, *Reuters* reported that Kaspersky Lab engaged in a "sabotage" campaign undoubtedly targeting the U.S. cybersecurity market.[4] Specifically, the company "tried to damage rivals in the marketplace by tricking their antivirus software programs into classifying benign files as malicious."[5] More recently, Russia's alleged interference in the 2016 presidential election has heightened public concerns about the Kremlin's desire to meddle with American democratic processes. This, in turn, has ignited speculation over America's cybersecurity posture, and the potential ties that Kaspersky Lab has with the Kremlin. Namely, that the Russian government could use products manufactured by Kaspersky Lab as a medium for engaging in nefarious cyber campaigns against U.S. information systems—including those at several federal departments and agencies—that are purportedly protected by the company's products.[6] Adding to concern, the FBI sent agents to visit "at least a dozen employees of Kaspersky" in order to question them "about the company's operations as part of a counter-intelligence inquiry."[7]

Given the increasing prevalence of cybersecurity threats across the nation, the federal government's use of cybersecurity products manufactured by a firm with potential ties to the Russian government is concerning to Congress. In May, the Senate Intelligence Committee held an open hearing where several top U.S. intelligence officials stated with consensus that they would not be comfortable using Kaspersky Lab's products on their systems.[8] Additionally, on June 15, 2017, the House Science Committee Subcommittees on Oversight and Research and Technology held a joint hearing where cybersecurity experts testified on industry approaches and

---

[3] Carol Matlack, *The Company Securing Your Internet Has Close Ties to Russian Spies*, BLOOMBERG BUSINESSWEEK, Mar. 19, 2015, *available at* https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies (last visited June 19, 2017).

[4] Joseph Menn, *Exclusive: Russian Antivirus Firm Faked Malware to Harm Rivals*, REUTERS, Aug. 14, 2015, *available at* www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QJ1CR20150814 (last visited June 27, 2017); *see also* Joseph Menn, *Exclusive: Russia's Kaspersky Threatened to 'Rub Out' Rival, Email Shows*, REUTERS, Aug. 28, 2015, *available at* http://www.reuters.com/article/us-kaspersky-rivals-idUSKCN0QX2GO20150828 (last visited June 27, 2017).

[5] *Id.*

[6] *See* Ali Watkins, *US Officials Are Warning About A Russian Cybersecurity Company's US Government Ties*, BUZZFEED NEWS, May 8, 2017, *available at* https://www.buzzfeed.com/alimwatkins/us-officials-are-warning-about-a-russian-cybersecurity?utm_term=.osyYrP2Mz6#.kexPnOw1Lk (last visited June 19, 2017); *see also* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).

[7] Ken Dilanian & Tom Winter, *Bill Would Bar Pentagon From Business With Russian Cyber Firm Kaspersky*, NBC NEWS, June 28, 2017, *available at* http://www.nbcnews.com/news/us-news/fbi-interviews-employees-russia-linked-cyber-security-firm-kaspersky-lab-n777571 (last visited June 29, 2017); *see also* Joe Uchill, *FBI Visits Kaspersky Lab Employees*, THE HILL, June 28, 2017, *available at* http://thehill.com/policy/cybersecurity/339887-fbi-visits-kaspersky-lab-employees (last visited June 29, 2017).

[8] S. Comm. on Intel., *Worldwide Threats Hearing*, 115th Cong. (May 11, 2017). (question and answer by Senator Marco Rubio).

best practices for safeguarding against future cyber threats.[9] Among the panel of expert witnesses was Salim Neino, CEO of Kryptos Logic—the cybersecurity firm whose employee helped thwart further propagation of the recent WannaCry ransomware attack.[10] In response to questions about the ability of a software manufacturer to embed a "backdoor" into anti-virus software—to facilitate a State's cyber-espionage activities—Mr. Neino alarmingly affirmed that he had "seen that a multitude of times" in the past, and that the barriers to engaging in such activities are "very low."[11] This revelation gives the Committee great concern, especially in light of the capabilities that anti-virus software possesses. Additionally, in response to a question regarding Kaspersky Lab, retired Army General Gregory Touhill, the first federal chief information security officer or CISO, told the Committee: "I buy American."[12]

Anti-virus software is extremely powerful and operates by scanning files at the system level, rather than on the network periphery.[13] As such, other security systems generally do not monitor the operations carried out by the anti-virus software.[14] From a practical perspective, this means that compromised anti-virus software could be used for malicious or nefarious purposes, and could do so without detection. If anti-virus technology or systems are compromised by a user's adversary, it could install malicious code disguised as a security update; it could forego specific updates to pave the way for use of certain vectors of attack; it could forego beneficial updates for a specified subset of users; and it could even extract data that a user's adversary considers valuable.[15] Furthermore, anti-virus is so powerful that it has nearly unimpeded access into all attachments, files, and information contained on a system.[16] In sum, compromised anti-virus has the potential to undermine the security and integrity of any system on which it is installed.

The security and integrity of federal information systems are only as strong as the products that guard them. Although Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, requires federal departments and agencies to implement the NIST Cybersecurity Framework and to provide reports related thereto,[17] the

---

[9] H. Comm. on Science, Space, & Tech. Subcomm. on Research & Tech. jointly with the Subcomm. on Oversight, *Hearing on Bolstering the Government's Cybersecurity: Lessons Learned from WannaCry*, Preliminary Hearing Transcript, 115th Cong. (June 15, 2017) at 61.
[10] *Id.*
[11] *Id.* at 62 (question and answer by Representative Clay Higgins).
[12] *Id.* at 63.
[13] *See* Joseph Marks, *The US Government Is Still Installing Russian Software on Its PCs*, DEFENSEONE, June 15, 2017, *available at* http://www.defenseone.com/technology/2017/06/us-government-still-installing-russian-software-its-pcs/138708/ (last visited June 19, 2017).
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] The White House, *Executive Order – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017), *available at* https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal (last visited June 29, 2017).

security of federal systems may nevertheless be undermined by compromised anti-virus products. Government contracting data indicating that several federal departments and agencies use or have used cybersecurity or anti-virus products manufactured by Kaspersky Lab is even more troubling.[18] If federal agencies and departments are being guarded by potentially compromised software, then it is virtually impossible for such agencies to effectively and efficiently implement the NIST Framework, and to fully comply with President Trump's executive order. The recent news that Kaspersky Lab's products have been removed from the General Service Administration's contracting Schedule 67 and 70 is encouraging, however federal agencies and contractors may be likely to continue use of Kaspersky Lab's products.[19]

Cybersecurity is a greater threat to our nation than ever before. If these widely reported allegations prove true, then the American public has ample grounds on which to rest their concerns about the security of data stored and transmitted on federal information systems—especially those allegedly protected by Kaspersky Lab's products. In light of this increasing threat, the Committee takes seriously its duty to ensure the NIST Cybersecurity Framework is properly equipped and adapted to safeguard our nation's information. To assist the Committee in understanding the effectiveness of the NIST Framework, and potential vulnerabilities that exist on federal information systems, please provide the following documents and information as soon as possible, but no later than August 11, 2017. Please provide the requested materials for the time frame from January 1, 2013, to present:

1. All documents and communications referring or relating to cybersecurity and/or anti-virus products manufactured by Kaspersky Lab.

2. All documents and communications referring or relating to any evaluation, risk assessment, and decision-making processes on the matter of whether to implement products manufactured by Kaspersky Lab.

3. All documents and communications referring or relating to the use or implementation of products manufactured by Kaspersky Lab.

---

[18] Government Contracting Dataset, *available at* https://www.usaspending.gov/Pages/AdvancedSearch.aspx?k=kaspersky (last visited June 29, 2017); *see* David Goldstein & Greg Gordon, *Exclusive: Kremlin Documents Suggest Link Between Cyber Giant and Russia Spy Agency*, MCCLATCHY, July 3, 2017, *available at* http://www.mcclatchydc.com/news/nation-world/national/article159342694.html (last visited July 12, 2017); *see also* Mike Levine & Pierre Thomas, *Officials Fear Russia Could Try To Target US Through Popular Software Firm Under FBI Scrutiny*, ABC NEWS, May 9, 2017, *available at* http://abcnews.go.com/US/officials-fear-russia-target-us-popular-software-firm/story?id=47295729 (last visited July 12, 2017).

[19] *See* Sarah Kuranda, *Kaspersky Lab Removed From GSA Schedule, Limiting Federal Sales for Its Security Software*, CRN, July 12, 2017, *available at* http://www.crn.com/news/security/300088591/kaspersky-removed-from-gsa-schedule-limiting-federal-sales-for-its-security-software.htm; *see also* Eric Geller, *Trump Administration Restricts Popular Russian Security Software*, POLITICO, July 11, 2017, *available at* http://www.politico.com/story/2017/07/11/trump-russian-security-software-240423.

4. A complete list of any computers, systems, data, media, and/or information utilizing or accessible to Kaspersky Lab products or services.

5. Identify any federal government contractors or subcontractors known to be utilizing Kaspersky Lab's products to fulfill requirements of contracts with the Department or Agency.

6. All documents and communications referring or relating to the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity.

7. All documents and communications referring or relating to the production of reports required by Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.

Pursuant to House Rule X, the Committee on Science, Space, and Technology has jurisdiction over National Institute of Standards and Technology which develops cybersecurity standards and guidelines for the federal government and recommendations for the private sector.

When producing documents to the Committee, please deliver production sets to the Majority Staff in Room 2321 of the Rayburn House Office Building and the Minority Staff in Room 394 of the Ford House Office Building. The Committee prefers, if possible, to receive all documents in electronic format.

If you have any questions about this request, please contact Drew Colliatie or Tom Connally at 202-225-6371. Thank you for your attention to this matter.

Sincerely,

Lamar Smith
Chairman

cc: The Honorable Eddie Bernice Johnson, Ranking Minority Member