UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

KASPERSKY LAB, INC. and KASPERSKY LABS LIMITED Plaintiffs, v. U.S. DEPARTMENT OF HOMELAND SECURITY and KIRSTJEN NIELSEN, in her official capacity as Secretary of Homeland Security Defendants.	) Civ. Act. No. 17-cv-02697-CKK

DECLARATION OF GRANT SCHNEIDER

I, Grant Schneider, do hereby declare and state:

1. I am the Acting Federal Chief Information Security Officer ("CISO") at the Office of Management and Budget ("OMB"). As the Acting Federal CISO, I oversee the development of government-wide cybersecurity policy and Federal civilian agency implementation of cybersecurity laws and policies. I also lead the Federal CISO Council, the primary body for collaboration and communication between Federal agency CISOs.

2. I was the Chief Information Officer ("CIO") for the Defense Intelligence Agency ("DIA") from 2007 to 2014, the Federal Cybersecurity Advisor for OMB from October 2014 to June 2015, and the Senior Advisor to the Acting Director of the Office of Personnel Management from June 2015 to January 2016, among other prior positions. As the CIO for DIA, I was

responsible for supporting the information technology ("IT") needs of more than 250,000 end users across 20-25 agencies in more than 140 countries. I oversaw the acquisition, development, installation and operations of enterprise, mission, and business IT systems. In this capacity I was responsible for DIA's compliance with federal, Department of Defense, and Intelligence Community information and information security requirements. Additionally, this included evaluating supply chain security risks for DIA IT acquisitions.

3. I make the statements in this Declaration based on my personal knowledge and experience and my evaluation of information furnished to me in the course of my official duties.

4. In my role as Acting Federal CISO, I engage regularly with federal executive branch agencies, including agency CIOs and agency CISOs, on a wide range of matters, including the security of federal information and information systems and supply chain security risks to such information and information systems. In my previous experience as a CIO and in my current role as Acting Federal CISO, I have become familiar with the rules and principles that govern procuring federal IT.

5. I am aware of DHS's issuance and implementation of binding operational directive ("BOD") 17-01, *Removal of Kaspersky-Branded Products*. I understand that a significant majority of federal agencies did not identify Kaspersky-branded products on their federal information systems, and of the federal agencies that did identify such products, nearly all have since removed those products and discontinued their use. I also am aware of Section 1634 of the National Defense Authorization Act for FY 2018, which goes into effect on October 1, 2018. Section 1634 prohibits federal government use of any hardware, software, or services developed or provided by Kaspersky. Based on conversations that I have had with CIOs and CISOs at individual agencies, federal agencies are widely aware of the NDAA prohibition and

are assessing the efforts that will be required to comply with the prohibition. Under the NDAA prohibition, all federal agencies must determine how they will identify and remove any Kaspersky hardware, software, or services currently in use on their information systems and remove the products before the October 1, 2018 statutory deadline. In addition, the NDAA requires that the Secretary of Defense, in consultation with other agencies, conduct a review of the procedures for removing suspect products or services from the IT networks of the federal government, and submit a report to congressional committees on the review in June 2018. In light of the NDAA prohibition, even if BOD 17-01 were rescinded before October 1, 2018, no federal agency would be likely to procure, test, and install Kaspersky products, and then remove them, all before the October 1st NDAA effective date.

6. By way of background, each federal agency makes its own independent IT acquisition decisions as long as the agency complies with applicable law and executive branch policy. These decisions often involve personnel with experience in IT, security, procurement, budget/finance, and other personnel. Depending on the value and significance of the acquisition, this can include the CIO, Chief Acquisition Officer, and other senior agency officials. The specific personnel and internal decision-making processes vary between the agencies, but all agencies are acutely aware of the need to avoid use of IT products that increase risks to their information and information systems. Under the Federal Information Security Modernization Act of 2014 ("FISMA"), the head of each federal agency is responsible for ensuring that the agency provides adequate information security protections to agency information and information systems. *See* 44 U.S.C. § 3554. This includes assessing security risks to information and information systems, "cost-effectively" reducing such risks to an acceptable level, ensuring information security is addressed throughout the life cycle of information

systems, and complying with OMB policies and procedures. *See* 44 U.S.C. § 3554(a), (b). These responsibilities need to be complied with before an agency procures software to install on its systems. Executive Order 13800, issued in May 2017, underscores the Federal government's renewed emphasis on agency accountability in this area, holding agency heads accountable to the President for implementing risk management measures commensurate with applicable risks and for ensuring that cybersecurity risk management processes are aligned with strategic, operational, and budgetary planning processes. Furthermore, a key OMB policy document, OMB Circular A-130, requires that agencies develop and implement a plan, or multiple plans, to address supply chain risks to agency information and communication technologies, as described in NIST Special Publication 800-161, to ensure the integrity, security, and resilience of federal information systems. *See, e.g.*, Appendix I-5.

7. Rescinding the BOD would not eliminate the security concerns underlying the decision to issue the directive in the first place. Those security concerns have been raised by numerous lawmakers and intelligence officials over the past year, and the enactment of the NDAA prohibition reflects a congressional judgment that those risks are too significant to ignore. Before purchasing Kaspersky software, agency procurement officials would have to confront these security concerns and determine, based on all available information, that using Kaspersky software in the months before the prohibition takes effect presents acceptable risks to the security or integrity of their networks. In these circumstances, if I was still an agency CIO, I could not reasonably accept the risk presented by the installation of Kaspersky products on my agency's information systems, and I find it highly unlikely that any other official would make a contrary decision.

8. In addition to the security risks, it would be wasteful to purchase software knowing its use will soon be prohibited. Agency CIOs have a legal obligation to manage resources in a prompt, efficient, and effective manner.[1] A wasteful procurement decision also could expose the agency to potential audit or investigation—whether by the agency's Office of the Inspector General, the General Accountability Office, or a congressional oversight committee.

9. Acquiring Kaspersky software only to remove it months later (i.e., by October 1, 2018) would be costly, inefficient, and inexcusably wasteful. Substituting one antivirus software for another across an entire agency's network requires considerable money and resources, above and beyond what it costs to license the software itself.

10. In addition to the costs and efforts associated with testing, installing, and integrating new software, pursuant to FISMA and based specifically on OMB Circular A-130, agencies are required to complete an "Authorization to Operate" ("ATO") before using an information system operationally and to conduct a reauthorization when the agency intends to make a change "likely to affect the security or privacy state of an information system." *See* OMB Circular A-130 at Appendix I-7, I-21 – I-22. Based on my knowledge and experience, substituting one anti-virus solution for another across an enterprise environment is a change that is likely to affect the security or privacy state of an information system. Accordingly, an agency choosing to install and then remove a Kaspersky product by October 1st would likely have to perform at least two reauthorizations: the first to switch to the Kaspersky product and the second to authorize the product that will replace it. I find it unlikely that an information security official would choose to go through these ATO efforts, in addition to the need to test, install, deploy, and

[1] *See, e.g.*, 44 U.S.C. § 3506(a)(3); OMB Circular A-130 (requiring agencies to "perform[] information resource management activities in an efficient, effective, economical, secure, and privacy-enhancing manner.")

remove the software, all before October 1st. Apart from being very difficult to justify on its own terms, such an undertaking would divert the time and energy of agency personnel who would be otherwise occupied with other IT and cybersecurity efforts. If the relevant information system were operated by a contractor, additional contractual, fiscal, and technical challenges would need to be addressed.

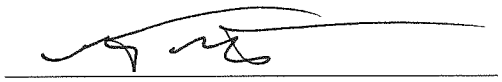
11. Finally, any new investment in Kaspersky software would frustrate agency efforts to bring their information systems in compliance with the NDAA. It would be wasteful for an agency to purchase and install Kaspersky software into their information systems while at the same time expending resources to identify and remove Kaspersky software embedded into third party products. As noted, the NDAA prohibition goes above and beyond the Kaspersky-branded products covered by the BOD, extending to "any hardware, software, or services" developed by Kaspersky. This broader prohibition covers not only the two Kaspersky services that were carved out of the BOD, but also any Kaspersky software embedded in the products of other companies. Identifying and removing Kaspersky products from third-party software will present considerable challenges, both because of the difficulty of determining whether Kaspersky software is integrated into the products of other companies used by an agency and also because of the technical and financial implications of removing and replacing any products identified. To comply fully, agencies will need to identify every single specific hardware device and software application on their networks, which could be hundreds or thousands of products, and determine whether each contains any Kaspersky software.

12. In light of the NDAA prohibition and the security, waste, procurement, fiscal, and technical factors described above, if BOD 17-01 were rescinded, I find it inappropriate for any agency to purchase and install Kaspersky software. I would discourage any agency to purchase

or install Kaspersky products before October 1st. If I was an agency CIO, I also would not recommend the purchase of such products before October 1st.

I declare under penalty of perjury that the foregoing is true and correct.

Executed in Washington, DC on February 5, 2018.



Grant Schneider