Written Testimony

Jeanette Manfra
Assistant Secretary for Cybersecurity and Communications
National Protection and Programs Directorate
U.S. Department of Homeland Security

Before the
U.S. House of Representatives
House Committee on Science, Space, and Technology
Oversight Subcommittee

Implementation of the Department of Homeland Security (DHS) Binding Operational Directive (BOD) 17-01 - Kaspersky Lab Software

November 14, 2017

Good morning Mr. Chairman, Ranking Member, and distinguished Members of the Subcommittee. Thank you for your interest in this important issue and the opportunity to provide an update on the Department's position regarding the Federal government's use of Kaspersky Lab (KL) software. I am the Assistant Secretary for Cybersecurity and Communications within the DHS National Protection and Programs Directorate (NPPD). NPPD executes many of the Department's authorities related to cybersecurity of federal networks.

The Federal Information Security Modernization Act of 2014 (FISMA) authorizes DHS to develop and oversee the implementation of binding operational directives (BODs), that are consistent with Office of Management and Budget (OMB) policies as well as National Institute of Standards and Technology (NIST) standards, to federal departments and agencies. FISMA defines a BOD as a "compulsory direction to an agency that is for purposes of safeguarding federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk." Federal agencies are required to comply with these DHS-developed directives.

A priority of DHS is to ensure the integrity and security of U.S. government systems, and in doing so must safeguard federal government systems by reducing potential vulnerabilities, protecting against cyber intrusions, and anticipating future threats.

On September 13, 2017, DHS Acting Secretary Elaine Duke signed BOD 17-01 to address the use of Kaspersky products, solutions, and services on federal information systems. After consultation with interagency partners, DHS determined Kaspersky products present a known or reasonably suspected information security risk to federal information systems. The BOD directs agencies to identify the use of these products within 30 days, provide a plan to remove them within 60 days, and, unless directed otherwise by DHS based on new information, to begin removing products at 90 days.

The Secretary's decision to issue the BOD is based on expert judgments about risks to federal information and information systems, which directly impact U.S. national security. In a public statement, the Department explained that it is concerned about (1) the ties between certain Kaspersky officials and Russian intelligence and other government agencies, (2) requirements under Russian law that allow Russian intelligence agencies to request or compel assistance from Kaspersky and to intercept communications transiting Russian networks, and (3) the broad access to files and elevated privileges provided by anti-virus products and services, including Kaspersky products, that can be exploited by malicious cyber actors to compromise information systems. The decision to use an anti-virus product is an information security risk decision ultimately based in trust. Given the ties between the company and Russian government agencies, the structure of the law in Russia, and the broad access that these products and services have, the Department lacks the necessary trust to allow the deployment of these products and services on

federal information systems. The action taken is a reasonable, measured approach to the information security risks posed by these products.

DHS is providing an opportunity for Kaspersky and any other entity that claims its commercial interests will be directly impacted by the BOD to submit to DHS a written response and any additional information or evidence supporting the response, to explain the adverse consequences, address the Department's concerns, or mitigate those concerns. DHS will review any submissions closely. As indicated in the BOD, DHS may provide other direction to federal agencies, based on new information, before the 90 day mark when agencies are to begin implementing the agency's plan of action to remove and discontinue use of Kaspersky products.

Thank you for the opportunity to testify today and I look forward to your questions.