STATEMENT BY

MS. ESSYE B. MILLER

DEPARTMENT OF DEFENSE (DOD)

DEPUTY CHIEF INFORMATION OFFICER (CIO) FOR CYBERSECURITY

BEFORE THE

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY OVERSIGHT SUBCOMMITTEE

ON

“Bolstering the Government’s Cybersecurity:

A Survey of Compliance with the DHS Directive”

NOVEMBER 14, 2017

NOT FOR PUBLICATION UNTIL RELEASED BY THE HOUSE SCIENCE, SPACE, AND TECHNOLOGY COMMITTEE, OVERSIGHT SUBCOMMITTEE

Introduction

Good morning Mr. Chairman, Ranking Member, and distinguished Members of the Subcommittee. Thank you for this opportunity to testify before the Subcommittee today on the Department's position regarding the Federal government's use of Kaspersky Lab (KL) software.

I am Essye B. Miller, a member of the Senior Executive Service. I currently serve as the Deputy Chief Information Officer (CIO) for Cybersecurity at the Department of Defense (DoD). Additionally, I serve as the Department's Chief Information Security Officer (CISO). My primary responsibility is to ensure that the Department maintains a well-defined and executed cybersecurity program. I am responsible for coordinating cybersecurity standards, policies and procedures with federal agencies, coalition partners and industry.

As the Assistant Secretary of Defense for Legislative Affairs stated in his letter to the full Committee in September, the Department agrees with the assessment that trustworthiness and integrity of information technology performing cybersecurity functions is an important matter.

In an unclassified setting, I can reiterate that as a matter of DoD enterprise cybersecurity, antivirus software (AV) does play a role. However, KL is not part of the DoD's antivirus solution. DoD has enterprise licenses for McAfee and Symantec antivirus, for both DoD devices and for DoD personnel home computer use. Kaspersky Lab Antivirus software (KL AV) is not on the DoD approved products list, nor do we have any contract awards listed for this software in our Federal Procurement Data System.

Although the Department of Homeland Security (DHS) Binding Operational Directive (BOD) 17-01 “Removal of Kaspersky-Branded Products” does not apply to statutorily defined "National Security Systems" nor to certain systems operated by the DoD, the Department has implemented the intent of the Directive. Prior to the BOD's release, on August 3, 2017, Joint Force Headquarters-DoD Information Network (JFHQ-DODIN) issued Task Order 17-0207 KASPERSKY ACTIVITY to mitigate threats to the DODIN potentially posed by adversaries leveraging KL products installed on DODIN infrastructure. Within the bounds of the BOD's requirements, we conducted a search of DoD's systems and confirmed that we did not have the listed Kaspersky products on any of our systems.

While KL does not present the sort of problem for DoD that it may for other components of the Federal government, it remains an ongoing supply chain risk management (SCRM) problem. If the DoD operates untrusted hardware or software, whether performing cybersecurity functions or not, within its systems or networks, there is the risk that those systems and networks can be compromised.

In order to reduce these risks, DoD issued DoD Instruction 5200.44, “Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)” (November 12, 2012). The instruction outlines a multi-discipline approach to supply chain risk management, integrating systems engineering, SCRM, security, counterintelligence, intelligence, cybersecurity, hardware and software assurance, assured services, and information systems security engineering. The policy, which applies to national security systems (NSS), establishes the DoD policy to identify mission critical functions and components, use all source intelligence analysis of the suppliers of critical components to inform risk management decisions, and apply risk management practices throughout the lifecycle, beginning in the design phase through the sustainment and operations phases.

To implement these policies in the Department, DoD has established and implemented the following processes and enterprise resources:

- A criticality analysis process, which identifies a system’s mission capabilities, mission-critical functions, and system components associated with those functions, and allocates criticality levels to those components. This process allows a program to focus attention and resources on the system’s most critical functions and components.

- A SCRM Threat Analysis Center (TAC) in the Defense Intelligence Agency (DIA) to provide supply chain threat assessments to programs on critical components.

- The Joint Federated Assurance Center (JFAC) to manage sharing of hardware and software (HW/SW) assurance testing capabilities and foster improved HW/SW test research and development. The JFAC Steering Committee is made up of representatives from the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)), DoD CIO, the Military Departments, Defense Information Systems Agency (DISA), National Security Agency (NSA), Missile Defense Agency (MDA), National Reconnaissance Office (NRO), Defense Microelectronics Activity, and the Department of Energy.

- A Trusted Systems and Networks (TSN) Roundtable, which meets quarterly with Service and Agency SCRM Focal Points and other stakeholders and supports DoD-wide implementation of DoDI 5200.44, by sharing SCRM/TSN best practices and defining TSN-enterprise capability requirements. For example, the TSN Roundtable developed a TSN Mitigations Playbook to share best practices on how to mitigate a wide variety of supply chain threats and vulnerabilities. The TSN Roundtable has also shared best practices on criticality analysis process as it applies to the networks/information systems environment and prioritization of Requests for Information from the SCRM TAC.

To assist the interagency, DoD has also worked through the Committee on National Security Systems (CNSS), to issue the CNSS Directive 505, “Supply Chain Risk Management,” which was recently updated. The Directive responds to challenges associated with SCRM and provides requirements for the U.S. Government to implement and sustain SCRM capabilities for NSS. This Directive (CNSSD No. 505) provides guidance for organizations while providing a "whole of government approach," resulting in enhanced inter-agency collaboration and the sharing of lessons learned to address SCRM.

DoD also co-chairs with DHS, the National Institute for Standards and Technology (NIST), and General Services Administration (GSA) the Software and Supply Chain Assurance Forum, a public-private forum bringing together industry-academia-government software assurance and supply chain risk management experts on a quarterly basis to share industry developments and best practices.

Conclusion

DoD recognizes the importance of the trustworthiness and integrity of information technology performing cybersecurity functions. The Department appreciates the support of the Subcommittee on these important matters and I would be happy to provide additional classified details on this issue in the appropriate setting. Thank you for the opportunity to testify today and I look forward to your questions.