HOLD FOR RELEASE
UNTIL PRESENTED
BY WITNESS
Nov. 14, 2017

Statement of
Reneé Wynn
Chief Information Officer
National Aeronautics and Space Administration

before the

Subcommittees on Oversight
Committee on Science, Space and Technology
U.S. House of Representatives

Chairman LaHood and Ranking Member Beyer, and Members of the Subcommittee, thank you for the opportunity to testify before you today regarding NASA's efforts to comply with a recent Binding Operational Directive (BOD) issued by the U.S. Department of Homeland Security (DHS) with regard to Kaspersky Lab-branded products. As NASA's Chief Information Officer (CIO), effectively managing and protecting the Agency's information technology (IT) resources in an ever-changing threat landscape is my number one priority.

Currently about 17,100 civil servants and 40,000 contractors work at nine NASA Centers and one Federally Funded Research and Development Center, as well as several smaller satellite facilities. We also collaborate with other international space agencies and have deep partnerships with researchers, engineers and scientists all over the world. Each day, hundreds of thousands of NASA personnel, contractors, academics and members of the public access some part of NASA's IT infrastructure – a complex array of information systems with more than 160,000 components geographically dispersed around the globe and beyond. This infrastructure plays a critical role in every aspect of NASA's mission, from controlling spacecraft to processing scientific data.

In support of NASA's many missions, the Office of the Chief Information Officer (OCIO) works to ensure that NASA's IT systems and their associated components are safeguarded from attack, assessed against stringent Federal and Agency security requirements, and are continuously monitored for compromise and for the effectiveness of currently implemented security measures. Given the evolving threat of attacks, our work is never done. Internal governance and infrastructure changes at NASA have already improved the Agency's security posture, but admittedly, more work remains, especially as the Agency evolves from a highly decentralized IT environment controlled by the Centers and Agency programs and projects to an enterprise IT environment that is more centrally managed and overseen by the Agency CIO.

NASA regularly conducts network scans on its internal, corporate network, mission operations networks, and provisioned guest networks. Corporate and mission networks are used to process Government data for official NASA business operations. Guest networks are for official, authorized NASA visitors and are not used to conduct NASA business or transmit Government data. NASA monitors systems connecting to its guest networks for improper use and malicious activity but it does not have complete insight into the system's hardware configurations or software inventory. To mitigate potential risk from these external systems, guest networks are designed as untrusted networks that have no privileged access to NASA data.

Additionally, the collective actions of NASA's OCIO, as well as information sharing with the DHS and other Federal agencies involved in cybersecurity, are contributing to an improved security posture. When threats are detected, NASA incident response personnel take immediate action, and depending on the level of the threat, NASA alerts other Federal agencies involved with cyber intelligence issues, and partners with them to deter and thwart future attacks.

Key Events

With regard to today's hearing topic, NASA would like to stress that Kaspersky Lab software is not part of the Agency's enterprise-licensed, core-load anti-virus software. Instead, since 2010, NASA has used Symantec Endpoint Protection as its core-load anti-virus solution under our End User Service contract. Therefore, the existence of any alternative anti-virus software on Agency hardware is considered to be a violation of Agency IT standards and will be immediately removed or its usage blocked unless a specific waiver is on file based on a risk assessment performed by the NASA OCIO -- the Agency's sole authority for NASA IT, to include IT risk acceptance.

Between Jan. 1, 2013 and mid-August 2017, NASA OCIO identified a small number of machines (work stations and mobile devices) which had Kaspersky Lab software installed on them and which were authorized to and did connect to NASA's internal network. This number included third-party international partners / bring your own device users. It is important to note that the NASA Office of Procurement has no record of Agency funds being used to purchase individual instances of Kaspersky Lab software, which leads officials to believe that the limited instances of Kaspersky Lab software found to exist on Agency hardware were likely the result of larger procurements and bundled services which included Kaspersky Lab software for free on purchased hardware. However, again, I must stress that the existence of Kaspersky Lab software or the existence of any non- Symantec anti-virus software on Agency hardware is a violation of Agency IT standards unless a waiver is granted by the CIO or her delegate.

On Sept. 13, 2017, NASA received DHS BOD-17-01 which required Federal and Executive branch departments and agencies to take action with regard to Kaspersky branded products on Federal IT systems. To comply with the BOD, departments and agencies were required to respond to DHS and to take specified actions within 30 and 60 days of, and at 90 days after, the BOD's issuance. Since receiving the BOD, NASA OCIO has identified no active installations of Kaspersky-branded products on devices or systems within the scope of BOD 17-01. NASA OCIO continues to leverage deployed continuous monitoring tools and regular incident response activities across NASA Centers to review and validate that Kaspersky Lab products are not appearing on the NASA network.

Also of note, in 1993, NASA was requested by the Government Services Agency (GSA) to be the pilot for the concept of Government-Wide Acquisition Contracts (GWAC). Subsequently, the Office of Management and Budget designated three agencies: NASA, the National Institutes of Health and GSA to provide GWAC vehicles for the use of acquiring IT products and services by the entire Federal Government. NASA's Solutions for Enterprise Wide Procurement (SEWP)[1] contract database then became the Agnecy's GWAC vehicle and as such supported acquisitions by NASA and the rest of the Federal Government. In July 2017, in coordination with the GSA and other major Government-wide contract vehicles, all offerings of Kaspersky Labs software were removed from NASA's SEWP contract

[1] The NASA SEWP Program Office operates under the Goddard Space Flight Center's CIO Office. Software and hardware is added by the various contract holders to provide the various Government agencies with offerings that the contract holders want to make available for purchase. There are currently 140 contract holders with products and services from 5500 manufacturers/software companies

database. Additionally Kaspersky Labs was de-activated as a legitimate provider for any future items being added to the SEWP contracts to avoid any possibility that items would be re-added later.

NASA Cybersecurity Environment

Before I conclude my testimony, I would like to speak briefly about NASA's cyber threat environment and our constant efforts to improve how we manage and protect our IT resources.

Decades of NASA aeronautics and space technology research and development represents billions of dollars in U.S. Government and aerospace industry investment. The very nature of NASA's mission, and the extremely important technical and intellectual capital produced therein, makes the Agency's information a valuable target for hackers, criminals and foreign enterprises. Many of these threats are well-resourced, highly motivated, and exhibit varying levels of sophistication. Therefore, there is no perfect, one-size-fits-all tool to predict, counter and mitigate the wide range of attacks across the Federal Government. However, new cybersecurity management tools are allowing NASA and other Federal agencies to have better insight into their networks, providing improved pro-active monitoring and mitigation of threats before they cause significant harm. For example, as part of NASA's implementation of the DHS Continuous Diagnostic Management (CDM) tool, NASA is transitioning in the near term to a unified vulnerability reporting dashboard structure. Full capability expected to be available in Fiscal Year 2018, as CDM phase 1 is completed in accordance with the DHS CDM implementation schedule. CDM Phase 1 will provide the following enhanced capabilities to the NASA continuous monitoring program:

- Hardware Asset Management: Using a tool to perform network discovery of all devices connected to any NASA owned or managed internet protocol address space, categorize the detected devices and monitor those devices;
- Software Asset Management: Using several tools to perform software inventory of all supported end-user devices, implement software whitelisting capability, monitor use of authorized and unauthorized software, and report software patch status for all supported end-user device;
- Configuration Settings Management: Using a tool to automate scanning of the U.S. Government Configuration Baseline and NASA configuration baseline settings and to decrease the time to scan for vulnerabilities; and
- Vulnerability Management: Using a tool establish configuration policies and automate network vulnerability scanning, and using the CDM Dashboard to enhance visibility.

Conclusion

In conclusion, protecting, better managing and upgrading NASA's IT infrastructure is and will remain a top Agency priority. When threats such as unauthorized software are detected, NASA personnel take immediate action to contain the threat. NASA is fully committed to becoming more secure, effective and resilient, and we are actively pursuing this on all levels.

Thank you for the opportunity to testify before you today, and I would be happy to answer any questions that you may have.