10/25/2017 Hearing: Cybersecurity Posture
The Oversight Subcommittee of the
Committee on Science, Space, and Technology of the
U.S. House of Representatives

Introduction

Good morning Chairman LaHood, Ranking Member Beyer, and members of the Subcommittee. My name is David Shive, and I am the Chief Information Officer (CIO) of the U.S. General Services Administration (GSA). I welcome the opportunity to share my organization's experiences related to the cybersecurity posture of the Federal Government, specifically pertaining to the utilization of Kaspersky Lab products at Federal agencies, as well as the implementation of Executive Order 13800 and the NIST Cybersecurity Framework.

GSA Mission

The mission of GSA is to deliver the best value in real estate, acquisition, and technology services to Government and the American people. GSA's priorities are to deliver better value and savings, serve our partners, expand opportunities for small business, make Government more sustainable, and be a leader in innovation.

In support of that, and as it relates to the Subcommittee's objectives today, one of my organization's key goals in supporting GSA's mission is to deliver technology that provides a secure environment for doing business, while ensuring that both IT and business continue to run efficiently.

FISMA

The Federal Information Security Modernization Act of 2014 (FISMA) provides a comprehensive framework which helps Federal CIOs and Federal Chief Information Security Officers (CISOs) manage overall Information Technology (IT) security risks across Federal data and assets.

The FISMA framework supports the rigorous IT security program implemented at GSA by the CISO under the auspices of the CIO's authority. Our security program assures risks to GSA's IT systems are assessed and proper security controls implemented to mitigate those risks down to an acceptable level. It also provides a comprehensive policy, procedure, and governance structure, and ensures periodic evaluation and testing of the effectiveness of IT security controls, including management, operational, and technical controls. Further, all GSA employees take IT security awareness training; role-based training may also be required dependent on position and function.

Furthermore, GSA has a robust incident handling and response program that strongly aligns with the NIST Cybersecurity Framework. Due to the effectiveness of that program, GSA received a rating of Level 4 (Managed and Measurable) under “Response” on the latest FISMA report from the Office of Inspector General (OIG).

NIST Standards, FISMA and ATOs

In accordance with FISMA, GSA adheres to all of NIST’s Federal Information Processing Standards (FIPS) and Special Publications (SP) in implementing GSA’s IT security program. These include standards and guidance on encryption, security categorization of confidentiality, integrity, and availability (i.e., low, moderate, high), security control selection and implementation, risk management, authentication, identity management, system authorization, and contingency planning.

In addition, GSA completes a risk-based security assessment in accordance with NIST guidance and issues a signed Authority to Operate (ATO) by the authorizing official with concurrence by the CISO before any new system goes into production. The ATO is the official declaration that the IT systems can go live and be operated within an acceptable level of risk.

Cybersecurity Risk Management

Using the FISMA framework, along with NIST’s Cybersecurity Framework, standards, and publications, GSA implements a risk-based strategy to manage IT security across the enterprise. Risk can never be completely eliminated, but the goal of GSA’s IT security program is to allow GSA to provide services to its customers using information technology operated within an acceptable level of risk. This is accomplished by prioritizing the implementation of the security controls and focusing on those that have the biggest impact on securing the system and data. These include, but are not limited to: encryption, 2-factor authentication, ensuring secure configurations and patching of vulnerabilities, access controls, and auditing and monitoring.

Implementation of EO 13800 and the NIST Cybersecurity Framework

GSA is in the process of implementing Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017). GSA has adopted the framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by the National Institute of Standards and Technology, as required by the Executive Order. Specifically, GSA uses the Identify, Protect, Detect, Respond, and Recover areas of the NIST cybersecurity framework to better manage the overall risk to the agency.

In addition, GSA has provided a risk management report, as well as an action plan to implement the Framework, to the Secretary of Homeland Security and the Director of the Office of Management and Budget (OMB) per the Executive Order. The report identified GSA’s highest risk areas along with risk mitigation and acceptance choices. GSA’s program received an overall evaluation of “Managing Risk” by the U.S. Department of Homeland Security (DHS) in their Cybersecurity Risk Management Assessment as part of the Executive Order.

GSA continues to explore leading edge technologies in order to stop the latest and most sophisticated attacks from our adversaries. These include next generation anti-virus solutions that use machine learning and artificial intelligence, as well as advanced detection of malware that is embedded in email attachments and links. This is done by doing in-depth analysis of the email before it reaches the end user. Both of these technologies will greatly protect the end user which is one of the primary vectors for exploiting Federal Government systems (otherwise known as phishing attacks).

GSA Role in Governmentwide IT Procurement

One of GSA’s core missions is to assist in procuring goods and services that can be made available to Federal agencies. GSA’s Federal Acquisition Service (FAS) offers a continuum of Governmentwide innovative solutions and services in a number of areas. Federal agencies spend approximately $23 billion annually to acquire IT products and services through FAS. This amount represents only 42 percent of the $54.8 billion in total contracted Federal IT spending across the entire Federal Government. As this figure indicates, Federal agencies are not required to use GSA contracts and, in fact, the majority of Federal IT spending does not occur through GSA.

Regardless of the acquisition vehicle used to acquire IT, as CIO it is my responsibility, as is the responsibility of any agency CIO, to ensure that we conduct a thorough examination of the IT solution and understand the risk of the product before we interface it with the existing agency IT infrastructure.

Significantly, a product’s placement on a GSA Multiple Award Schedule (Schedule) or other contract vehicle only certifies that the vendor meets the necessary contract and legal authority requirements for the product to be sold to the Federal Government; it does not make any value or technical judgment about the nature of the product. In the IT space, FISMA requires agency CIOs, such as myself, to make the determination for which products and solutions are appropriate for an agency’s environment.

With respect to Kaspersky Lab (KL) products, three resellers offered KL products through GSA Schedules contracts, but did not gain approval to do so via the required contract modification process. On July 11, 2017, GSA directed the three resellers to remove all KL manufactured products from their catalogs within 30 days. All three resellers complied. In addition, it is GSA’s understanding that on the same day, NASA and NIH, the other two Federal agencies with Governmentwide IT procurement contracts, removed Kaspersky manufactured products from their resellers’ catalogs. GSA does not offer any Kaspersky Lab manufactured products through its Schedules contracts.

Discovery and Removal of Kaspersky Products

GSA took a proactive stance and completed comprehensive scanning of all IT assets for the presence of KL products in June 2017. GSA confirmed that there was no installation of KL products in GSA's on-premise and cloud-based systems, and reported this to DHS in accordance with its Binding Operational Directive (BOD) 17-01 on October 4, 2017. GSA currently uses McAfee as its anti-virus provider.

In addition, GSA's Federal Risk and Authorization Management Program's (FedRAMP) Program Management Office is coordinating this activity for the Governmentwide Cloud Service Providers (CSPs) that are covered by FedRAMP ATOs.

Conclusion

Again, I thank you for allowing me the opportunity to contribute to this important topic. GSA appreciates this Committee's oversight of the Federal Government's cybersecurity posture on behalf of the American people.

At this time, I'm happy to take any questions that you might have.