UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

**STATEMENT OF
THE HONORABLE
KATHERINE ARCHULETA
DIRECTOR
U.S. OFFICE OF PERSONNEL MANAGEMENT**

before the

**SUBCOMMITTEE ON FINANCIAL SERVICES AND GENERAL GOVERNMENT
COMMITTEE ON APPROPRIATIONS
UNITED STATES SENATE**

on

"A Review of IT Spending and Data Security at OPM"
**---
June 23, 2015**

Chairman Boozman, Ranking Member Coons, and Members of the subcommittee:

Government and non-government entities are under constant attack by evolving and advanced persistent threats and criminal actors. These adversaries are sophisticated, well-funded, and focused. Unfortunately, these attacks will not stop – if anything, they will increase. Although OPM has taken significant steps to meet our responsibility to secure the personal data of those we serve, it is clear that OPM needs to dramatically accelerate these efforts, not only for those individuals personally, but also as a matter of national security. When I was sworn in as the Director of the U.S. Office of Personnel Management (OPM) 18 months ago, I immediately became aware of security vulnerabilities in the agency's aging legacy systems and I made the modernization and security of our network and its systems one of my top priorities. My goal as Director of OPM, as laid out in OPM's February 2014 *Strategic Information Technology (IT) Plan*, has been to leverage cybersecurity best practices to protect the sensitive information entrusted to the agency, while modernizing our IT infrastructure to better confront emerging threats and meeting our mission and customer service expectations.

Strengthening and Enhancing OPM's Data Security

Over the last eighteen months, OPM has undertaken an aggressive effort to update its cybersecurity posture, adding numerous tools and capabilities to its networks. For Fiscal Years (FY) 2014 and 2015 we have committed nearly $70 million towards shoring up our IT infrastructure. In June 2014, we began to completely redesign our current network, while also protecting our legacy network to the maximum extent possible in the interim. These projects are ongoing, on schedule, and on budget. The first phase of this project was to deploy the tools required to address critical vulnerabilities on the existing network. As part of this effort, in January 2015 we implemented state of the art practices, such as additional firewalls, two-factor authentication for remote access, and limited privileged access rights. Currently, we are also increasing the types of methods utilized to encrypt our data. These methods cover not only data at rest, but data in transit, and data displayed through masking or redaction.

As a result of these efforts to improve our security posture, in April 2015, an intrusion that predated the adoption of these security controls affecting OPM's IT systems and data was detected by our new cybersecurity tools. OPM immediately contacted the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) and, together with these partners, initiated an investigation and forensic analysis to determine the scope and impact of the intrusion. Shortly thereafter, OPM notified Congressional leadership and select committees of this incident. In early May, the interagency incident response team shared with relevant agencies that the exposure of personnel records had occurred. That very same day, we worked to brief Congressional leadership and select committees. In early June, OPM informed Congress and the public that notifications would be sent to affected individuals beginning on June 8 through June 19. We refer to this incident as the intrusion affecting personnel records.

As part of the ongoing investigation and analysis, we are continuing to learn more about the systems that contributed to individuals' data potentially being compromised. For example, we have now confirmed that any Federal employee from across all branches of government whose organization submitted service history records to OPM may have been compromised – even if their full personnel file is not stored on OPM's system. These individuals were included in the previously identified population of approximately four million current and former Federal employees and are being appropriately notified.

During the course of the ongoing investigation, the interagency incident response team concluded – later in May – that additional systems were likely compromised, also at an earlier date. In late May, OPM and the interagency notified Congressional leadership and select committees of this separate intrusion. This separate incident – which also predated deployment of our new security tools and capabilities – continues to be investigated by OPM and our interagency partners. Based on this continuing investigation, in early June, the interagency response team shared with relevant agencies that there was a high degree of confidence that OPM systems related to background investigations of current, former, and prospective Federal government employees, and those for whom a federal background investigation was conducted, may have been compromised. We are currently working with our interagency partners to continue to offer classified briefings for Members and staff on the status of this investigation. While we have not yet determined its scope and impact, we are committed to notifying those individuals whose information may have been compromised as soon as practicable. This separate incident is one that we refer to as the intrusion affecting background investigations.

But for the fact that OPM implemented new, more stringent security tools in its environment, we would have never known that malicious activity had previously existed on the network, and would not have been able to share that information for the protection of the rest of the Federal Government. In response to these incidents, OPM, working with our partners at DHS has immediately implemented additional security measures to protect the sensitive information it manages and to take steps toward building a simplified, modern, and flexible network infrastructure.

<u>Driving Continued Progress on IT Modernization</u>

We continue to execute on our aggressive plan to modernize OPM's platform and bolster security tools. We are on target to finish a completely new modern and secure data center environment by the end of FY 2015 which will eventually replace our legacy network. OPM's 2016 budget request included an additional $21 million above 2015 funding levels to further support the modernization of our IT infrastructure, which is critical to protecting data from the persistent adversaries we face. This funding will help us sustain the network security upgrades and maintenance initiated in FY2014 and FY2015 to improve OPM's cyber posture, including advanced tools such as database encryption and stronger firewalls and storage devices.

Conclusion

As we are all aware, Government and non-government entities are under constant attack by evolving and advanced persistent threats and criminal actors. Again – we recognize that these attacks will increase. We are working with an interagency team to identify and rapidly implement protections that will decrease our risk; however, as we address critical immediate needs we also need to continue our work to address long-term strategic challenges that affect our ability to ensure the security of our networks in light of this persistent threat. As our OIG has noted, OPM has been challenged for several years in building and maintaining a strong management structure and the processes needed for a successful information technology security program. OPM agrees with this assessment which is why I prioritized development of the agency's *Strategic IT Plan* and have prioritized its implementation.

We discovered these intrusions because of our increased efforts in the last eighteen months to improve cyber security at OPM, not despite them. I am dedicated to ensuring that OPM does everything in its power to protect the federal workforce, and to ensure that our systems will have the best cyber security posture the government can provide.

We thank you for your support of our ongoing efforts to strengthen our IT security and I appreciate the opportunity to testify today. I am happy to address any questions you may have.