UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

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

before the

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
UNITED STATES HOUSE OF REPRESENTATIVES

on

"OPM: Data Breach"

June 16, 2015

Chairman Chaffetz, Ranking Member Cummings and Members of the committee:

When I was sworn in as the Director of the U.S. Office of Personnel Management (OPM) 18 months ago, I recognized that in order to meet our goals to build and manage an engaged, inclusive, and well-trained workforce that we would need a thorough assessment of the state of information technology (IT) at OPM. When I was sworn in I said that I would develop an IT strategic plan in my first 100 days and delivered on that promise in February 2014. 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 IT Plan*, is to innovate IT infrastructure at OPM in a way that leverages cybersecurity best practices and protects the sensitive information entrusted to the agency.

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. In an average month, OPM, for example thwarts 10 million confirmed intrusion attempts targeting our network. These attacks will not stop – if anything, they will increase. I'm here today to talk to you

about two successful intrusions that were detected recently but took place in the past. I'm also here to deliver a message to Federal employees, retirees, and their families: the security of your personal data is of paramount importance. We are committed to a full and complete investigation of these incidents and are taking action to mitigate vulnerabilities exposed by intrusions.

Strengthening and Enhancing OPM's Cybersecurity

As I stated earlier, within the last year, OPM has undertaken an aggressive effort to update its cybersecurity posture, adding numerous tools and capabilities to its networks. We are focused on protecting our legacy network to the maximum extent possible as we design a more modern system. As part of these efforts, we have improved network monitoring and logging capability to contain intrusions and ensure data is protected. Additional firewalls were installed in the network to better segment systems and data, and enhanced authentication for remote access is being enforced.

As a result of our 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. 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 intrusion as the intrusion affecting personnel records.

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 – remains under investigation by OPM and our interagency partners. 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. OPM and its interagency partners have briefed the House Permanent Select Committee on Intelligence on their preliminary findings and FBI Director Comey briefed the Senate Select Committee on Intelligence. 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 the Department of Homeland Security (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.

Driving Continued Progress on IT Modernization

We continue to execute on our aggressive plan to modernize OPM's platform and bolster security tools. OPM's 2016 budget request includes 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 cyberposture, including advanced tools such as database encryption, stronger firewalls and storage devices, and masking software. The funding will also support the redesign of OPM's legacy network.

Conclusion

In conclusion, I want to emphasize that cyber security issues that the Government is facing is a problem that has been decades in the making, due to a lack of investment in federal IT systems and a lack of efforts in both the public and private sectors to secure our internet infrastructure. We discovered these intrusions because of our increased efforts in the last eighteen month 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.

Thank you for this opportunity to testify today and I am happy to address any questions you may have.