UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

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

before the

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

on

"Under Attack: Federal Cybersecurity and the OPM Data Breach"

June 25, 2015

Chairman Johnson, Ranking Member Carper, and Members of the committee:

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 OPM's IT Security

First, I would like to address confusion regarding the number of people affected by the two recent, related cyber incidents at OPM.

It is my responsibility to provide as accurate information as I can to Congress, the public, and most importantly, the affected individuals. Second, because this information and its potential misuse concerns their lives, it is essential to identify the affected individuals as quickly as possible. Third, we face challenges in analyzing the data due to the form of the records and the way they are stored. As such, I have deployed a dedicated team to undertake this time consuming analysis and instructed them to make sure their work is accurate and completed as quickly as possible. As much as I want to have all the answers today, I do not want to be in a position of providing you or the affected individuals with potentially inaccurate data.

With these considerations in mind, I want to clarify some of the reports that have appeared in the press. Some press accounts have suggested that the number of affected individuals has expanded from 4 million individuals to 18 million individuals. Other press accounts have asserted that 4 million individuals have been affected in the personnel file incident and 18 million individuals have been affected in the background investigation incident.

Therefore, I am providing the status as we know it today and reaffirming my commitment to providing more information as soon as we know it.

First, the two kinds of data I am addressing - - personnel records and background investigations - - were affected in two different systems in two recent incidents.

Second, the number of individuals with data compromised from the personnel records incident is approximately 4.2 million, as we reported on June 4. This number has not changed, and we have notified these individuals.

Third, as I have noted, we continue to analyze the background investigation data as rapidly as possible to best understand what was compromised, and we are not at a point where we are able to provide a more definitive report on this issue.

That said, I want to address the figure of 18 million individuals that has been cited in the press. It is my understanding that the 18 million refers to a preliminary,

unverified and approximate number of unique social security numbers in the background investigations data. It is not a number that I feel comfortable, at this time, represents the total number of affected individuals. The social security number portion of the analysis is still under active review, and we do not have a more definitive number. Also, there may be overlap between the individuals affected in the background investigation incident and the personnel file incident. Additionally, we are working deliberately to determine if individuals who have not had their social security numbers compromised, but may have other information exposed, should be considered individuals affected by this incident. For these reasons, the 18 million figure may change. My team is conducting this further analysis with all due speed and care, and again, I look forward to providing an accurate and complete response as soon as possible.

I also want to share with this committee some new steps that I am taking. First, I will be hiring a new cybersecurity advisor that will report directly to me. This cybersecurity advisor will work with OPM's CIO to manage ongoing response to the recent incidents, complete development of OPM's plan to mitigate future incidents, and assess whether long-term changes to OPM's IT architecture are needed to ensure that its assets are secure. I expect this individual to be serving the agency by August 1. Second, to ensure that the agency is leveraging private sector best practices and expertise, I am reaching out to Chief Information Security Officers at leading private sector companies that experience their own significant cybersecurity challenges and I will host a meeting with these experts in the coming weeks to help identify further steps the agency can take to protect its systems and information. As you know, the public and private sector both face these challenges, and we should face them together.

In March 2014, we released our *Strategic Information Technology Plan* to modernize and secure OPM's aging legacy system. The focus of the Plan is a set of strategic initiatives that will allow OPM to administer IT with greater efficiency, effectiveness, and security. This work recognizes recommendations from the U.S. Government Accountability Office and OPM's Office of Inspector General (OIG). Work to implement the Plan began immediately, and in Fiscal Years (FY) 2014 and 2015 we re-prioritized critical resources to direct nearly $70 million toward the implementation of tough new security controls to better protect our systems. OPM is also in the process of developing a new network infrastructure environment to improve the security of OPM infrastructure and IT systems. Once completed, OPM IT systems will be migrated into this new environment from the current legacy networks.

Many of the improvements have been to address critical immediate needs, such as the security vulnerabilities in our network. These upgrades include the installation of additional firewalls; restriction of remote access without two-factor authentication; continuous monitoring of all connections to ensure that only legitimate connections have access; and deploying anti-malware software across the environment to protect and prevent the deployment or execution of cyber-crime tools that could compromise our networks. These improvements led us to the discovery of the malicious activity that had occurred, and we were able to immediately share the information so that other agencies could protect their networks.

OPM thwarts millions of intrusion attempts on its networks in an average month. We are working around the clock to identify and mitigate security weaknesses. The reality is that integrating comprehensive security technologies into large, complex outdated IT systems is a lengthy and resource-intensive effort. It is a challenging reality, but one that we are determined to address. We have implemented these tools to the maximum extent possible, but the fact is that we were not able to deploy them before these two sophisticated incidents, and, even if we had been, no single system is immune to these types of attacks.

As we address critical immediate needs we also need to continue our work to improve long-term strategic challenges that affect our ability to ensure the security of our networks. I view the relationship that OPM has with our Inspector General as collaborative. We appreciate their recommendations and take them very seriously. 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 and it is this weakness that the Strategic IT Plan was developed to resolve.

I also want to discuss the important issue of data encryption. Though data encryption is a valuable protection method, today's adversaries are sophisticated enough that encryption alone does not guarantee protection. OPM does currently utilize encryption when possible; however, due to the age of some of our legacy systems, data encryption is not always possible. In fact, I have been advised by security experts that encryption in this instance would not have prevented the theft of this data, because the malicious actors were able to steal privileged user credentials and could decrypt the data. Our IT security team is actively building

new systems with technology that will allow OPM not only to better identify intrusions, but to encrypt even more of our data. Currently, we are increasing the types of methods utilized to encrypt our data.

In addition to new policies that were already being implemented to centralize IT security duties under the Chief Information Officer (CIO) and to improve oversight of new major systems development, the Plan recognized that further progress was needed. Thanks to OPM CIO Donna Seymour's leadership, the OIG's November 2014 audit credited OPM for progress in bolstering information technology security policies and procedures, and for committing critical resources to the effort.

Where the audit found weaknesses in Information Security Governance and Security Assessment and Authorization, OPM was already planning and implementing upgrades that emphasized improved security and the adoption of state of the art security protocols. Once these upgrades reached a mature stage in the spring of 2015, we were able to detect earlier intrusions into our data. Cybersecurity is fundamentally about risk management, and we must ensure that any recommendation helps us achieve the most effective level of cybersecurity and at the same time, allows us to continue providing critical services to the Federal workforce.

With regard to Information Security Governance, the OIG noted that OPM had implemented significant positive changes and removed its designation as a material weakness. This was encouraging, as IT governance is a pillar of the Strategic IT Plan. An enhanced IT governance capacity will identify and ensure we fund IT investments that are more tightly aligned with our needs. It will also allow us to manage, evaluate, measure, and monitor IT services in a more consistent and repeatable manner.

Regarding the weaknesses found with Security Assessment and Authorization, the OIG had recommended that I consider shutting down 11 out of 47 of OPM's IT systems because they did not have a current and valid Authorization. I am the leader of an organization that provides critical services to over two million current Federal employees around the world. The legacy systems that we are aggressively updating are critical to the provision of those services. Shutting down systems would mean that retirees would not get paid, and that new security clearances could not be issued. I am dedicated to ensuring that OPM does everything in its power to protect the federal workforce. But part of that included ensuring that our

retirees receive the benefits they have earned and federal employees get the healthcare they need.

Of the systems raised in the FY 2014 audit report, eleven of those systems were expired. Of those, one, a contractor system, is presently expired. All other systems raised in the FY 2014 audit report have been either extended or provided a limited Authorization.

Addressing Federal Employees' Needs

For those approximately 4 million current and former Federal civilian employees who were potentially affected by the incident announced on June 4 regarding personnel information, OPM is offering credit monitoring services and identity theft insurance with CSID, a company that specializes in identity theft protection and fraud resolution. This comprehensive, 18-month membership includes credit report access, credit monitoring, identity theft insurance, and recovery services and is available immediately at no cost to affected individuals identified by OPM.

The high volume of notifications sent on the 18th and 19th of June, along with the a significant number of calls being made to the CSID call center from individuals who have not been impacted or notified of impact, caused wait times to increase, and those selecting on-line sign up at the end of last week experienced the CSID site timing out.

Our team is continuing to work with CSID to make the online signup experience quicker and to reduce call center wait times. These actions involve expanded staffing and call center hours, and increasing server capacity to better handle on-line sign ups at peak times. We continue to update our FAQ's on opm.gov to address questions that we are getting from individuals who have or feel they may have been impacted.

Conclusion

The OIG's assessments of OPM's plans reflected the difficulties involved in working with complex legacy systems. This type of assessment is helpful to ensure OPM has the best, most comprehensive plans possible, and the OIG report helps everyone, including Congress, understand that these are complex issues that will require significant resources, both time and funding, to correct.

I would like to emphasize again that OPM has taken steps to ensure that greater restrictions are in place, even for privileged users. This includes removing remote access for privileged users and requiring two-factor authentication. We are looking into further protections, such as tools that mask and redact data that would not be necessary for a privileged user to see.

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