United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

June 10, 2015

The Honorable Katherine Archuleta
Director
U.S. Office of Personnel Management
1900 E St., NW
Washington, DC 20415

Dear Ms. Archuleta:

The Homeland Security and Governmental Affairs Subcommittee on Regulatory Affairs and Federal Management is conducting oversight on the recent Office of Personnel Management data breach. This breach raises significant concerns as to the security of OPM's information technology (IT) systems and the integrity of its data management.

The integrity of OPM's IT systems underpins the agency's ability to provide administrative and personnel services to the federal workforce, which in turn is essential to the basic functioning of the federal government. OPM has repeatedly characterized the security of its IT systems as a high-priority issue, and has within the past year "undertaken an aggressive effort to update its cybersecurity posture,"[1] with plans to "innovate IT infrastructure . . . in a way that protects the sensitive information entrusted to us by the Federal workforce and the American people."[2]

It is therefore extremely concerning that on June 4, 2015, officials announced that OPM's computer systems were hacked, compromising the personally identifiable information of millions of federal workers.[3] Even more troubling, although the hack was the "the largest breach of federal employee data in recent years,"[4] it was not the first: OPM's systems were discovered

---

[1] Press Release, Office of Personnel Mgmt., OPM to Notify Employees of Cybersecurity Incident (June 4, 2015).
[2] *Enhancing Cyber Security of Third-Party Contractors and Vendors: Hearing Before the H. Comm. on Oversight & Gov't Reform*, 114th Cong. (Apr. 22, 2015) (written testimony of Donna Seymour, Chief Info. Officer, Office of Personnel Mgmt.).
[3] Ellen Nakashima, *Chinese Breach Data of 4 Million Federal Workers*, WASH. POST (June 4, 2015), http://www.washingtonpost.com/world/national-security/chinese-hackers-breach-federal-governments-personnel-office/2015/06/04/889c0e52-0af7-11e5-95fd-d580f1c5d44e_story.html.
[4] *Id.*

to have been breached in March 2014, and two OPM contractors, U.S. Investigations Services (USIS) and KeyPoint Government Solutions, were discovered to be hacked in 2014.[5]

OPM's inconsistent responses to the USIS and KeyPoint breaches only deepen our concern of OPM's ability to self-assess the security of its internal IT systems, which were likely similarly vulnerable, and which have resulted in a breach significantly more devastating. In response to the self-reported USIS breach, which exposed 25,000 federal employees' personally identifiable information, OPM went so far as to suspend work with the company and eventually cut all ties with USIS.[6] In contrast, OPM merely gave KeyPoint a slap on the wrist for a breach which comprised 48,000 federal employees, and which was only detected by the Department of Homeland Security.[7] At the time, OPM issued a statement promising that "KeyPoint has worked closely with OPM to implement additional security controls that will afford its network greater protection."[8] That OPM would so disparately reprimand its contractors for their IT security, while failing to prevent a breach *fifty-five times larger* than the USIS and KeyPoint breaches combined, raises serious questions about the integrity of OPM's IT security.

As the Subcommittee charged with oversight of the federal workforce, I am extremely concerned about what is "among the largest known thefts of government data in history."[9] Understandably, much speculation and many questions remain. In order to address these concerns, the Subcommittee is conducting oversight of this matter which may lead to a public hearing. In order to understand the breadth of this data breach I ask that you please provide the following information:

1. On what date(s) did the breach announced June 4 ("the breach") occur, and for how long did it persist?
2. On what date did OPM learn of the breach? Please provide a chronology of OPM's investigation.
3. On what date did OPM fulfill its obligation under 44 U.S.C. § 3544(b)(7) to notify the Federal information security incident center of the breach?
4. On what date did OPM notify the Department of Homeland Security and the Federal Bureau of Investigations of the breach?

---

[5] Christian Davenport, *KeyPoint Network Breach Could Affect Thousands of Federal Workers*, WASH. POST (Dec. 18, 2014), http://www.washingtonpost.com/business/economy/keypoint-suffers-network-breach-thousands-of-fed-workers-could-be-affected/2014/12/18/e6c7146c-86e1-11e4-a702-fa31ff4ae98e_story.html/

[6] Camille Tuuttii & Jack Moore, et. al, *48,000 Federal Employees Potentially Affected by Second Background Check Hack*, NEXTGOV (Dec. 18, 2014), http://www.nextgov.com/cybersecurity/2014/12/opm-alerts-feds-second-background-check-breach/101622/.

[7] *Id.*

[8] *Id.*

[9] Devlin Barrett & Danny Yadron, et. al, *U.S. Suspects Hackers in China Breached About 4 Million People's Records, Officials Say*, WALL ST. J. (June 5, 2015), http://www.wsj.com/articles/u-s-suspects-hackers-in-china-behind-government-data-breach-sources-say-1433451888.

5. On what date did OPM notify affected individuals that their personally identifiable information had been compromised, and offer credit protection services?
6. OPM's press release states that the breach announced on June 4 "predated the adoption of the tougher security controls" adopted as part of OPM's cybersecurity reforms, and "[a]s a result" of OPM's updated cybersecurity capabilities, OPM was able to "detect[] a cyber-intrusion." Has OPM investigated whether or not additional breaches, perhaps "predat[ing] the adoption of" these capabilities, and which could only be detected with the updated capabilities, occurred? If so, what were the results of those investigations?
7. OPM officials have indicated that OPM will pay for credit monitoring services for all federal employees whose personally identifiable information has been compromised as a result of the breach. OPM has also indicated that it would provide up to $1 million in identity theft insurance for affected employees through CSID.
    a. How will OPM fund these efforts, and from which appropriated account(s)?
    b. On what date did OPM arrange with CSID to provide credit monitoring services?
    c. How did OPM identify CSID as a vendor? What procurement process was used?
8. Does OPM intend to revise its Strategic IT Plan in light of the security breaches within the agency over the past year, as well as those at its contractors? What additional remedial measures does OPM intend to take?
9. What individual or entity created the cybersecurity plan for OPM prior to the June 4, 2015 breach? What assurances did the individual or entity give to OPM of the plan's effectiveness?

Please provide your responses no later than **June 22, 2015 at 5:00 p.m.** If you have any questions about this request, please contact John Cuaderes with Chairman Lankford's staff at (202) 224-6704. Thank you for your attention to this matter.

Sincerely,

James Lankford
Chairman
Subcommittee on Regulatory Affairs and
Federal Management

cc: The Honorable Heidi Heitkamp
Ranking Minority Member
Subcommittee on Regulatory Affairs and Federal Management