

# United States Senate

WASHINGTON, DC 20510

June 23, 2015

The Honorable Shaun Donovan  
Director, U.S. Office of Management and Budget  
725 17<sup>th</sup> Street, N.W.  
Washington, D.C. 20503

The Honorable Jeh Johnson  
Secretary, U.S. Department of Homeland Security  
Nebraska Avenue Complex  
3801 Nebraska Avenue, N.W.  
Washington, D.C. 20528

The Honorable Katherine Archuleta  
Director, U.S. Office of Personnel Management  
1900 E Street, N.W.  
Washington, D.C. 20415

Dear Director Donovan, Secretary Johnson and Director Archuleta:

Over the last few weeks, I have been deeply troubled to learn the details of the successful cyberattacks on the Office of Personnel Management (OPM). Not only has sensitive information about millions of Americans been stolen, but we still do not know the full impact it will have on our national security. As your agencies prepare this week to testify in front of the Senate Homeland Security and Governmental Affairs Committee about the attacks, it is essential the Committee be given a full accounting of what happened.

Protecting our nation's secrets and most sensitive information is among the government's highest priorities and a vital component of its national security mission. Yet over the last five years, Americans have watched with growing concern as government records have been leaked or stolen by our adversaries. In 2010, then-Pfc. Bradley Manning handed over more than 700,000 classified documents and videos to the website *WikiLeaks* in what was called the biggest leak in U.S. military history.<sup>1</sup> He was surpassed in 2013 by Edward Snowden, who leaked thousands of pages detailing the operations of our intelligence programs at the National Security Agency.<sup>2</sup>

---

<sup>1</sup> Lewis, Paul, "Bradley Manning given 35-year prison term for passing files to WikiLeaks," *The Guardian*, August 21, 2013, <http://www.theguardian.com/world/2013/aug/21/bradley-manning-35-years-prison-wikileaks-sentence>.

<sup>2</sup> Kopan, Tal, "Ex-CIA chief Michael Hayden: Edward Snowden leak worse than Bradley Manning's," *Politico*, August 2, 2013, <http://www.politico.com/story/2013/08/michael-hayden-edward-snowden-bradley-manning-95113.html>.

And just this month we learned that hackers successfully breached the Office of Personnel Management and stole highly sensitive records related to millions of federal workers along with their friends, family and co-workers. Yesterday, *CNN* reported that in closed-door briefings, FBI Director James Comey told senators that 18 million Americans were affected by the OPM data breaches.<sup>3</sup> Some have called it the biggest cyberattack our government has ever suffered, though the full scope is still being investigated.

During the course of the investigation, however, a mix of reports coming both from federal officials and through the news media have offered incomplete, and at times conflicting, accounts of both the scale of the attacks as well as their impact. The urgency of the situation is too great to wait for details to trickle in. To the greatest extent possible, the administration needs to explain to the American public what it knows and what it means for them.

My intent with this letter is to summarize what is currently being reported about the OPM breaches in order to learn from you if it is accurate. By separating fact from fiction, I hope to clarify what we know, what we do not know, and what we need to do to act quickly in defense of our nation. When the entire picture is put together, the cyber events in and around OPM over the last 16 months raise three serious concerns for Americans, many of whom do not yet know the full extent of what happened.

The first is how these breaches will increase our vulnerabilities to terrorism and weaken our national security. We have only begun to absorb the implications of putting so much sensitive information about millions of federal employees and private citizens in the hands of our adversaries, and I fear it will only get worse.

The second is how much information was exposed, and the extent to which Americans have had their privacy violated. For many, no information is more closely held than one's own health history, yet the OPM breaches could mean uncertainty and fear for years to come.

Third, and finally, is the risk of identity theft and the potential costs to the economy. Identity theft costs our nation billions of dollars each year, not counting the time it takes to recover. Anyone who has had their identity stolen knows that it can take weeks to get your life back in order.

This week's hearing will focus primarily on two breaches into OPM's networks: one into its central personnel file, affecting more than four million current and former federal workers; and a second into its database containing security clearance background information on perhaps millions more federal workers.<sup>4</sup> However, a full picture of the problem requires examining a broader number of incidents, including OPM's long history of cybersecurity weaknesses.

In mid-March 2014, OPM first learned that hackers successfully breached its networks and were able to access files related to security clearance background checks in the Electronic

---

<sup>3</sup> Perez, Evan, and Shimon Prokupecz, "First on CNN: U.S. data hack may be 4 times larger than the government originally said," *CNN*, June 22, 2015, <http://www.cnn.com/2015/06/22/politics/opm-hack-18-million/>.

<sup>4</sup> Website of the Office of Personnel Management, Latest News (Announcements), "Frequently Asked Questions," June 18, 2015, <http://www.opm.gov/news/latest-news/announcements/frequently-asked-questions/>.

Questionnaires for Investigations Processing (e-QIP) system. The attack – unofficially attributed to the Chinese government – was unsuccessful, however, because the intrusion was detected and the attackers were removed from the network before they could take any data.<sup>5</sup>

How the March 2014 breach into the security clearance database blocked the hackers from removing data, however, is not publicly known, including whether the federal government’s cyber intrusion-detection system, EINSTEIN, played a role.

EINSTEIN protects federal civilian networks by looking for malicious Internet traffic and, when it is detected, blocks it. The system was first put in place in 2004 and has been rolled out in three phases through the years. EINSTEIN 1 was designed to measure information flows into and out of government networks. Several years later EINSTEIN 2 added the ability to detect intrusions from malicious actors, providing an early warning system. Finally, EINSTEIN 3A not only uses classified information to detect bad actors, but also blocks them from entering or exiting federal networks, as needed.

Despite having these capabilities, Dr. Andy Ozment, assistant homeland security secretary for cybersecurity at DHS testified to Congress last week that EINSTEIN 3A is still not in place at OPM, and was not at the time of the first successful attack.<sup>6</sup>

Around the same time as the OPM breach in March 2014, though, hackers also successfully breached U.S. Investigations Service, or USIS, a government contractor responsible at the time for handling roughly half of all federal security clearances. They were able to exfiltrate background investigation files related to security clearances for 25,000 employees at DHS, including those at its headquarters, at Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE).<sup>7</sup>

This attack was followed two months later in May by a breach into Premera Blue Cross, which participates in the Federal Employee Health Benefits Program (FEHBP). As many as 11 million people had their information exposed, including their “name, date of birth, Social Security number, mailing address, email address, telephone number, member identification number, bank account information, and claims information, including clinical information.”<sup>8</sup> Shortly after, CareFirst Blue Cross, another FEHBP participant, was breached, exposing an additional 1.1 million individuals, many of which were federal employees.<sup>9</sup> China was

---

<sup>5</sup> Schmidt, Michael S., David E. Sanger and Nicole Perlroth, “Chinese Hackers Pursue Key Data on U.S. Workers,” *The New York Times*, July 9, 2014, <http://www.nytimes.com/2014/07/10/world/asia/chinese-hackers-pursue-key-data-on-us-workers.html? r=0>.

<sup>6</sup> Hearing of the House Oversight and Government Reform Committee, “OPM: Data Breach,” June 16, 2015, <http://www.c-span.org/video/?326593-1/hearing-office-personnel-management-data-breach>.

<sup>7</sup> Finkle, Jim, and Mark Hosenball, “U.S. undercover investigators among those exposed in data breach,” *Reuters*, August 23, 2014, <http://www.reuters.com/article/2014/08/23/us-usa-security-contractor-cyberattack-idUSKBN0GM1TZ20140823>.

<sup>8</sup> Pepitone, Julianne, “Premera Blue Cross Hacked: 11 Million Customers Could Be Affected,” *NBC News*, March 17, 2015, <http://www.nbcnews.com/tech/security/premera-blue-cross-hacked-11-million-customers-affected-n325231>.

<sup>9</sup> Humer, Caroline, “CareFirst says cyberattack stole data of 1.1 million users in U.S.” *Reuters*, May 20, 2015, <http://www.reuters.com/article/2015/05/20/us-carefirst-cyberattack-idUSKBN0O52IF20150520>.

suspected in both instances,<sup>10</sup> and questions were raised about the possible connections to the OPM attacks.

While the two health care breaches would not be disclosed for many months, the USIS hack came to light much sooner. In June, USIS detected the intrusion from March, at which point it informed OPM – however, two months had already passed and significant damage was done. In response, DHS suspended USIS from processing any more security clearances and shifted much of the remaining work to two other contractors, CACI and KeyPoint.<sup>11</sup>

DHS officials at the time were quick to dismiss any public speculation about a link between the USIS attack and the attack on OPM, despite both having been unofficially attributed to China.<sup>12</sup> Yet, inside OPM, senior leaders were alarmed enough about their own breach that in April 2014 they launched an ambitious effort to overhaul and secure the agency’s entire information technology infrastructure. OPM’s inspector general had sounded a consistent warning that the agency’s IT systems were badly out of date and insecure since at least 2007, but until the March breach agency leaders demonstrated little urgency to act. It would eventually become apparent that OPM’s sudden lurch forward toward cybersecurity would prove costly, poorly planned and could possibly leave it in worse condition.<sup>13</sup>

The overhaul effort, however, would also prove far too little and too late. Sometime in June or July 2014, OPM’s networks would once again be breached, with hackers once again targeting the agency’s security clearance database, e-QIP. Only, where the last attack had been detected and blocked, this one was successful – and would also not be discovered for nearly a year.<sup>14</sup> Unofficial reports would also once again attribute the attack to the Chinese government.<sup>15</sup>

While the full scope of the attack is not yet known, hackers were able to steal enormous numbers of background security clearance files – known as Standard Form 86 – which contain hundreds of pages of sensitive information on those with security clearances. The forms contain not only detailed histories about an employee’s career, health and personal habits, but also information about friends, family members and neighbors.<sup>16</sup> “This is some of the most sensitive

---

<sup>10</sup> Mathews, Anna Wilde, and Danny Yadron, “Health Insurer CareFirst Says It Was Hacked,” *Wall Street Journal*, May 20, 2015, <http://www.wsj.com/articles/health-insurer-carefirst-says-it-was-hacked-1432149975>.

<sup>11</sup> Davenport, Christian, “USIS contracts for federal background security checks won’t be renewed,” *The Washington Post*, September 9, 2014, [http://www.washingtonpost.com/business/economy/opm-to-end-usis-contracts-for-background-security-checks/2014/09/09/4fcd490a-3880-11e4-9c9f-ebb47272e40e\\_story.html](http://www.washingtonpost.com/business/economy/opm-to-end-usis-contracts-for-background-security-checks/2014/09/09/4fcd490a-3880-11e4-9c9f-ebb47272e40e_story.html).

<sup>12</sup> Nakashima, Ellen, “DHS contractor suffers major computer breach, officials say,” *The Washington Post*, August 6, 2014, [http://www.washingtonpost.com/world/national-security/dhs-contractor-suffers-major-computer-breach-officials-say/2014/08/06/8ed131b4-1d89-11e4-ae54-0cfe1f974f8a\\_story.html](http://www.washingtonpost.com/world/national-security/dhs-contractor-suffers-major-computer-breach-officials-say/2014/08/06/8ed131b4-1d89-11e4-ae54-0cfe1f974f8a_story.html).

<sup>13</sup> Dilanian, Ken, “Flash audit: ‘Serious concerns’ about personnel computer fix,” *Associated Press*, June 19, 2015, <http://news.yahoo.com/flash-audit-serious-concerns-personnel-computer-fix-072440655--politics.html>.

<sup>14</sup> Website of the Office of Personnel Management, Latest News (Announcement), “Information About the Recent Cybersecurity Incidents,” June 18, 2015, <https://www.opm.gov/news/latest-news/announcements/>.

<sup>15</sup> Nakashima, Ellen, “Officials: Chinese had access to U.S. security clearance data for one year,” *The Washington Post*, June 18, 2015, <http://www.washingtonpost.com/blogs/federal-eye/wp/2015/06/18/officials-chinese-had-access-to-u-s-security-clearance-data-for-one-year/>.

<sup>16</sup> Website of the Office of Personnel Management, Standard Form 86, [https://www.opm.gov/forms/pdf\\_fill/sf86.pdf](https://www.opm.gov/forms/pdf_fill/sf86.pdf).

non-classified information I could imagine the Chinese getting access to,” later noted Stewart Baker, a former high-ranking official with DHS.<sup>17</sup>

By early September 2014, with USIS awaiting a final decision on its suspension from work on security clearance background investigations, DHS cancelled its contract with the company altogether. The temporary move to give the work to CACI and KeyPoint would become more permanent. In an email obtained by the *Washington Post*, OPM’s chief information officer, Donna Seymour, tried to reassure colleagues at the time that KeyPoint could be trusted to secure the massive new influx of files. “[F]ollowing the discovery of the problem, KeyPoint implemented numerous controls to strengthen the security of its network,” she wrote, “The immediacy with which KeyPoint was able to remediate vulnerabilities has allowed us to continue to conduct business with the company without interruption.”<sup>18</sup>

This assertion would quickly prove incorrect when in September, KeyPoint was also breached, exposing the information of nearly 50,000 federal employees.<sup>19</sup> Investigators were not immediately sure if any of the security clearance information that had been accessed was actually stolen.<sup>20</sup> Further investigation revealed that information from as many as 390,000 employees may have been compromised.<sup>21</sup>

Meanwhile, despite launching its IT overhaul project in April 2014, OPM’s cybersecurity weaknesses remained unfixed nearly seven months later. In November, the IG issued a year-end review of the agency’s cybersecurity and sounded the alarm. Not only was OPM unable even to inventory all of its “servers, databases and network devices,” but computer security agreements with contractors had expired and remote access to servers did not require “multi-factor authentication.”<sup>22</sup> The IG went so far as to recommend “shutting down systems” that did not have certified cybersecurity systems in place – two of which were responsible for holding security clearance information.<sup>23</sup>

---

<sup>17</sup> Nakashima, Ellen, “Officials: Chinese had access to U.S. security clearance data for one year,” *The Washington Post*, June 18, 2015, <http://www.washingtonpost.com/blogs/federal-eye/wp/2015/06/18/officials-chinese-had-access-to-u-s-security-clearance-data-for-one-year/>.

<sup>18</sup> Davenport, Christian, “KeyPoint network breach could affect thousands of federal workers,” *The Washington Post*, December 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](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).

<sup>19</sup> Davenport, Christian, “KeyPoint network breach could affect thousands of federal workers,” *The Washington Post*, December 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](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).

<sup>20</sup> Davenport, Christian, “KeyPoint network breach could affect thousands of federal workers,” *The Washington Post*, December 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](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).

<sup>21</sup> Caldwell, Alicia A., “390,000 People Tied to DHS May Have Had Data Breached,” *Associated Press*, June 15, 2015, <http://abcnews.go.com/Technology/wireStory/390000-people-tied-dhs-data-breached-31785477>.

<sup>22</sup> Final Audit Report of the U.S. Office of Personnel Management, Office of Inspector General, “Federal Information Security Management Act Audit, FY 2014,” Report Number 4A-CI-00-14-016, November 12, 2014, <https://www.opm.gov/our-inspector-general/reports/2014/federal-information-security-management-act-audit-fy-2014-4a-ci-00-14-016.pdf>.

<sup>23</sup> Final Audit Report of the U.S. Office of Personnel Management, Office of Inspector General, “Federal Information Security Management Act Audit, FY 2014,” Report Number 4A-CI-00-14-016, November 12, 2014, <https://www.opm.gov/our-inspector-general/reports/2014/federal-information-security-management-act-audit-fy-2014-4a-ci-00-14-016.pdf>.

The following month in December, OPM would again be hit with a successful cyberattack. This time, hackers accessed the agency's personnel files housed at the Department of the Interior.<sup>24</sup> Speculation about the target of the breach has centered on OPM's Central Personnel Data File<sup>25</sup> or its Electronic Official Personnel Folder system, the latter of which was housed at Interior.<sup>26</sup> These databases contain detailed personnel records on every current, and many former, federal employees, including "Social Security numbers, birthdays, addresses, military records, job and pay histories, and various insurance information, in addition to age, gender, and race data."<sup>27</sup> At a hearing last week of the House Oversight and Government Reform Committee, federal officials confirmed that not only was none of the stolen information encrypted, but that it also contained health insurance information on federal employees.<sup>28</sup>

Also in December, hackers successfully breached Anthem, one of the largest health insurance providers in the nation, which operates Blue Cross and Blue Shield Federal Employee Program.<sup>29</sup> One private cybersecurity company, iSight Partners, publicly linked the attack on Anthem to the attempted attack on OPM.<sup>30</sup> Eighty million Anthem customers had their information exposed in what was called the largest "medical-related cyber-intrusions in history."<sup>31</sup> This followed two attacks mentioned previously at Premera Blue Cross and CareFirst Blue Cross.

In March 2015, just four months after its scathing report on OPM's network security, the IG was once again surprised to learn about new cybersecurity problems inside the agency. During a series of budget meetings with agency leadership, the IG first discovered that OPM had launched its project to overhaul its IT infrastructure – now nearly a year underway.<sup>32</sup> Perhaps to shield itself from more criticism, OPM leadership had kept the IG in the dark about the project and proceeded without any of the usual oversight. In addition to its November report on OPM's

---

<sup>24</sup> Nakashima, Ellen, "Chinese breach data of 4 million federal workers," *The Washington 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](http://www.washingtonpost.com/world/national-security/chinese-hackers-breach-federal-governments-personnel-office/2015/06/04/889c0e52-0af7-11e5-95fd-d580f1c5d44e_story.html).

<sup>25</sup> Dilanian, Ken, "Union: Hackers have personnel data on every US gov't employee," *Associated Press*, June 11, 2015, <http://news.yahoo.com/union-hackers-personnel-data-every-us-govt-employee-195701976.html>.

<sup>26</sup> Gallagher, Sean, "'EPIC' fail – how OPM hackers tapped the mother lode of espionage data," *Ars Technica*, June 21, 2015, <http://arstechnica.com/security/2015/06/epic-fail-how-opm-hackers-tapped-the-mother-lode-of-espionage-data/>.

<sup>27</sup> Volz, Dustin, "OPM Hackers Stole Data on Every Federal Employee," *National Journal*, June 11, 2015, <http://www.nationaljournal.com/tech/opm-hackers-stole-data-on-every-federal-employee-20150611>.

<sup>28</sup> Hearing of the House Oversight and Government Reform Committee, "OPM: Data Breach," June 16, 2015, <http://www.c-span.org/video/?326593-1/hearing-office-personnel-management-data-breach>.

<sup>29</sup> Sternstein, Aliya, "Anthem Health Care Hack Snared Federal Employees Who Weren't Anthem Customers," *NextGov*, February 27, 2015, <http://www.nextgov.com/cybersecurity/2015/02/anthem-healthcare-hack-snared-federal-employees-who-werent-anthem-customers/106260/>.

<sup>30</sup> Nakashima, Ellen, "Chinese breach data of 4 million federal workers," *The Washington 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](http://www.washingtonpost.com/world/national-security/chinese-hackers-breach-federal-governments-personnel-office/2015/06/04/889c0e52-0af7-11e5-95fd-d580f1c5d44e_story.html).

<sup>31</sup> Harwell, Drew, and Ellen Nakashima, "China suspected in major hacking of health insurer," *The Washington Post*, February 5, 2015, [http://www.washingtonpost.com/business/economy/investigators-suspect-china-may-be-responsible-for-hack-of-anthem/2015/02/05/25fbb36e-ad56-11e4-9c91-e9d2f9fde644\\_story.html](http://www.washingtonpost.com/business/economy/investigators-suspect-china-may-be-responsible-for-hack-of-anthem/2015/02/05/25fbb36e-ad56-11e4-9c91-e9d2f9fde644_story.html).

<sup>32</sup> Memorandum from Patrick E. McFarland, Inspector General, U.S. Office of Personnel Management, to Katherine Archuleta, Director, U.S. Office of Personnel Management, "Flash Audit Alert - U.S. Office of Personnel Management's Infrastructure Improvement Project (Report No. 4A-CI-00-15-055), June 17, 2015.

poor cybersecurity, the IG had loudly criticized the agency for its attempt to do a similar upgrade on a single IT system. Now, OPM was attempting to overhaul nearly 50 IT systems at once – an immensely larger and more complicated effort that if not successful could leave OPM less secure than when it started.

By April, OPM would begin to understand the price our government would pay for its failures over many years. While upgrading its security systems, the agency, with the help of the FBI and DHS, finally detected the December 2014 breach.<sup>33</sup> Several weeks later in June OPM would also learn about the earlier successful breach in the June/July 2014 period into its security clearance database.<sup>34</sup> The latter breach had gone undetected for nearly a year while the second breach was discovered in-progress nearly five months after-the-fact.<sup>35</sup>

The extent of the damage done by these attacks is not yet fully known, nor is it fully known how quickly OPM has moved to address the most glaring problems. On June 18, OPM confirmed that information related to at least four million federal employees may have been stolen, including their “name[s], Social Security Numbers, dates of birth, and possibly other sensitive information.”<sup>36</sup> Regarding the June/July 2014 hack into the security clearance database, the agency simply said, “OPM, DHS, and the FBI are working as part of this ongoing investigation to determine the number of people affected by this separate intrusion.”<sup>37</sup> As already mentioned, the most recent report claims 18 million people were affected.

Moreover, it is not clear whether OPM’s decisions in the aftermath of the breaches have been effective to protect its networks going forward or whether it is moving fast enough. The IG has raised recent concerns on both counts. On June 17, the inspector general’s office issued a rare “flash audit” to OPM, warning the agency’s IT overhaul project was in perilous shape and could take years to complete. It said,

“OPM currently estimates that it will take 18 to 24 months to complete. We believe this is overly optimistic and that the agency is highly unlikely to meet this target. ... In our opinion, the project management approach for this infrastructure overhaul is entirely inadequate, and introduces a very high risk of project failure. ... In this scenario, the agency would be forced to indefinitely support multiple data centers, further stretching already inadequate resources, possibly making both environments less secure, and increasing costs to taxpayers.”<sup>38</sup>

---

<sup>33</sup> Website of the Office of Personnel Management, Latest News (Announcements), “Frequently Asked Questions,” June 18, 2015, <http://www.opm.gov/news/latest-news/announcements/frequently-asked-questions/>.

<sup>34</sup> Website of the Office of Personnel Management, Latest News (Announcements), “Frequently Asked Questions,” June 18, 2015, <http://www.opm.gov/news/latest-news/announcements/frequently-asked-questions/>.

<sup>35</sup> Gallagher, Sean, “Why the ‘biggest government hack ever’ got past the feds,” *Ars Technica*, June 8, 2015, <http://arstechnica.com/security/2015/06/why-the-biggest-government-hack-ever-got-past-opm-dhs-and-nsa/>.

<sup>36</sup> Website of the Office of Personnel Management, Latest News (Announcements), “Frequently Asked Questions,” June 18, 2015, <http://www.opm.gov/news/latest-news/announcements/frequently-asked-questions/>.

<sup>37</sup> Website of the Office of Personnel Management, Latest News (Announcements), “Frequently Asked Questions,” June 18, 2015, <http://www.opm.gov/news/latest-news/announcements/frequently-asked-questions/>.

<sup>38</sup> Memorandum from Patrick E. McFarland, Inspector General, U.S. Office of Personnel Management, to Katherine Archuleta, Director, U.S. Office of Personnel Management, “Flash Audit Alert - U.S. Office of Personnel Management’s Infrastructure Improvement Project (Report No. 4A-CI-00-15-055), June 17, 2015.

OPM responded to the IG yesterday, June 22, in a memo defending its IT overhaul project, saying it would take “the next several months” for OPM to determine the scope of the project.<sup>39</sup> And in response to concerns that the process for undertaking the project was badly flawed, Director Archuleta responded: “Regardless of its traditional or nontraditional nature, the procurement process followed by Department of Homeland Security (who serves as the contracting office) is compliant with applicable law.”<sup>40</sup> Nowhere in the memo did the director expressly respond to concerns raised by the IG that the project has a high rate of failure and could leave the agency less secure as a result.

In the continuing aftermath of the attacks, questions are also focused on how exactly the breaches happened. Regarding the December breach of personnel data, public reports suggest it may have been the result of a “spear fishing” incident followed by a “zero day” attack.<sup>41</sup> In this case, attackers sent an email to employees at Interior, who opened it and allowed the attackers to gain access to its systems housing OPM data. In the words of one analyst, “It’s similar to a thief slipping through a broken or unlocked window to get into a house.”<sup>42</sup>

Regarding the earlier breach into the security clearance system, *ABC News* cited concerns by those briefed on the investigation that the entry point into OPM may have been discovered in the September 2014 breach of KeyPoint.<sup>43</sup> Using information stolen in that attack, hackers are believed to have gained access to OPM’s systems.

One person, identified by *Ars Technica* only as a “consultant who did some work with a company contracted by OPM to manage personnel records,” claimed that OPM’s networks were vulnerable to Chinese hackers for years.

[H]e found the Unix systems administrator for the project “was in Argentina and his co-worker was physically located in the [People’s Republic of China]. Both had direct access to every row of data in every database: they were root. Another team that worked with these databases had at its head two team members with PRC passports. I know that because I challenged them personally and revoked their privileges. From my perspective, OPM compromised this information more than three years ago and my take on the current breach is ‘so what’s new?’”<sup>44</sup>

---

<sup>39</sup> Memorandum from Katherine Archuleta, Director, Office of Personnel Management, to Patrick E. McFarland, Inspector General, Office of Personnel Management, “Response to Flash Audit Alert – U.S. Office of Personnel Management’s Infrastructure Improvement Project (Report No. 4A-CI-00-15-055), June 22, 2015.

<sup>40</sup> Memorandum from Katherine Archuleta, Director, Office of Personnel Management, to Patrick E. McFarland, Inspector General, Office of Personnel Management, “Response to Flash Audit Alert – U.S. Office of Personnel Management’s Infrastructure Improvement Project (Report No. 4A-CI-00-15-055), June 22, 2015.

<sup>41</sup> Gallagher, Sean, “Why the ‘biggest government hack ever’ got past the feds,” *Ars Technica*, June 8, 2015, <http://arstechnica.com/security/2015/06/why-the-biggest-government-hack-ever-got-past-opm-dhs-and-nsa/>.

<sup>42</sup> Zetter, Kim, “Hacker Lexicon, What is a Zero Day?” *Wired*, November 11, 2014, <http://www.wired.com/2014/11/what-is-a-zero-day/>.

<sup>43</sup> Levine, Mike, and Jack Date, “Feds Eye Link to Private Contractor in Massive Government Hack,” *ABC News*, June 12, 2015, <http://abcnews.go.com/US/feds-eye-link-private-contractor-massive-government-hack/story?id=31717372>.

<sup>44</sup> Gallagher, Sean, “Encryption ‘would not have helped’ at OPM, says DHS official,” *Ars Technica*, June 16, 2015, <http://arstechnica.com/security/2015/06/encryption-would-not-have-helped-at-opm-says-dhs-official/>.

In light of these serious concerns, I believe it is essential the administration provide Congress and the American people with a full accounting of what is currently known. To that end, I would appreciate answers to the following questions.

1. Who is responsible for the cyberattacks on OPM in 2014?
2. How much information was stolen in the two known hacks?
3. How many people will ultimately be affected, including non-federal employees listed on Standard Form 86 files?
4. How many breach notification letters has OPM sent out? How many additional notifications does it plan to send out beyond the four million announced on June 4?
5. Why were notifications not sent out to those affected by the breaches until months after the administration became aware of them?
6. Have all known cyber intrusions been publicly reported?
7. Is the personnel datafile and the security clearance datafile now secure?
8. Are the hackers who exfiltrated data in the 2014 attacks out of our system now?
9. Other than those mentioned in this letter, have the hackers responsible for the attacks on OPM ever attempted another known attack on federal networks? If so, when and what was the result?
10. Are there any federal agency networks operating today with known “material weaknesses” in their cyber defenses?
11. Do any other federal agencies operate with the kind of decentralized control over their IT systems that OPM was using prior to being breached? If so, which ones and why?
12. Why does EINSTEIN 3A not cover all civilian federal agencies?
13. How did OPM detect and block an intrusion into OPM’s security clearance database in March 2014?
14. Why was OPM unable to detect and block an intrusion on the same database in the June/July 2014 cyberattack?
15. Why did EINSTEIN not catch the outflow of data related to the breaches of both the personnel files as well as the security clearance background information files?

16. When did the government launch its “30-day cybersecurity sprint” and what is it intended to accomplish?
17. Did the Department of the Interior host sensitive information from any other agency than OPM?
18. Were the breaches at OPM related to the breaches at Anthem, Premera Blue Cross and Carefirst Blue Cross?
19. How are the attacks on USIS, KeyPoint and OPM related?
20. What level of cybersecurity is required of federal contractors? Who is responsible for ensuring they comply?
21. Has OPM completed a full inventory of all servers and databases? If not, why not and when will it be completed?
22. In Director Archuleta’s memo last night she said it would take “the next several months” to assess the full scope of its “Migration” process. Precisely how long do you estimate this process will take?
23. Did the breach on OPM result in the exfiltration of information from members of the military, intelligence community or contractors?
24. Director Archuleta on June 17 told the House Oversight and Government Reform Committee, “It is not feasible to [encrypt] networks that are too old.” Why?
25. Did any of OPM’s failures to properly secure maintain its information technology networks permit either of the breaches in 2014?
26. Prior to knowing about the breaches, how did OPM measure whether it was successfully achieving cybersecurity?
27. Is anyone to blame for this failure? If so, how does the administration believe they be held accountable?

As a member of the Senate Homeland Security and Governmental Affairs Committee, I take seriously my oversight responsibilities and appreciate you working with me to answer to these important questions.

Sincerely,



Ben Sasse  
U.S. Senator