JASON CHAFFETZ, UTAH
CHAIRMAN

ONE HUNDRED FOURTEENTH CONGRESS

ELIJAH E. CUMMINGS, MARYLAND
RANKING MINORITY MEMBER

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225-5074
MINORITY (202) 225-5051

http://oversight.house.gov

MEMORANDUM

September 6, 2016

To: Democratic Members of the Committee on Oversight and Government Reform

Fr: Democratic Staff

Re: Committee Investigation into the OPM Data Breach

Tomorrow, Wednesday, September 7, 2016, Chairman Chaffetz will release a report, drafted by the Republican staff, setting forth their conclusions from the Committee's investigation into cyber attacks against the Office of Personnel Management (OPM). Unfortunately, Ranking Member Cummings could not support this report because of several key deficiencies.

First, the Republican staff report fails to adequately address federal contractors and their role in federal cybersecurity. The most significant deficiency uncovered during the Committee's investigation was the finding that federal cybersecurity is intertwined with government contractors, and that cyber requirements for government contractors are inadequate. The evidence obtained by the Committee demonstrated that:

- a "well-planned campaign" by a sophisticated adversary targeted both OPM and private sector contractors for the government;
- sensitive information about federal employees was stolen from both OPM and private sector companies performing services for the government;
- the OPM breach was achieved using credentials taken from one of OPM's contractors to disguise its initial movements into and through OPM's computer network; and
- contract requirements for sharing information with private sector companies that handle sensitive government data need strengthening.

Second, the Republican staff report unfairly criticizes former Chief Information Officer (CIO) Donna Seymour. Even before the Committee began its investigation, Chairman Chaffetz demanded Ms. Seymour's resignation, and he called for her resignation on at least five occasions. The Republican staff report repeats assertions made by Chairman Chaffetz, but ignores specific evidence refuting them. Specifically:

- OPM discovered the breach with tools deployed by Ms. Seymour, and claims that a private company conducting a product demonstration was responsible for discovering the intrusion are inaccurate.

- The specific justifications used by Chairman Chaffetz for demanding Ms. Seymour's resignation were not supported by the evidence obtained by the Committee.

I. CYBER OFFICIALS BELIEVE OPM DATA BREACH WAS RELATED TO BREACHES OF CONTRACTOR COMPUTER NETWORKS

Beginning in March 2014, and continuing over a 12-month period, OPM detected two breaches of its computer network. The first breach did not result in the theft of personally identifiable information (PII).[1] The second breach, which was detected around the time that efforts to remediate the first breach were complete, resulted in the loss of sensitive background investigations data on more than 22 million people, including federal employees who applied for, received, or currently possess security clearances. The stolen information contained PII, including fingerprints, as well as information on family members, neighbors, and friends.

A. Top Cyber Officials Concluded OPM Breach Was Part of a "Well-Planned Campaign and High Level of Sophistication" That "Systematically Attacked Those Entities All at the Same Time"

On June 5, 2015, the National Cybersecurity and Communications Integration Center within the Department of Homeland Security (DHS) issued a report entitled "Large-Scale PII Breach Incidents." The report stated:

> US-CERT is aware of approximately nine major security incidents in which PII was stolen from private sector companies, U.S. government agencies, and a cleared defense contractor. The cyber threat actors involved in each of these incidents demonstrated a well-planned campaign and high level of sophistication.[2]

In a transcribed interview with Committee staff, Jeff Wagner, OPM's Director of IT Security Operations, stated:

> OPM is knowledgeable of multiple direct correlations between OPM and its subcontractors, whether it is a health insurance contractor, such as Anthem or Blue Cross,

---

[1] Department of Homeland Security, *OPM Incident Report* (June 22, 2014).

[2] Department of Homeland Security, *Analysis Report* (June 5, 2015).

or whether it's a [Federal Investigative Service] contractor for OPM, such as USIS or KeyPoint, but it would be hard to say that it was simply a coincidence that OPM was attacked as well as many of its subcontracts.

He also said of the OPM attackers: "they systematically attacked those entities all at the same time."[3]

B. OPM Attackers Also Targeted Private Companies, Including Anthem

Cyber officials' name for the intrusion set responsible for the OPM breach is "Cold Cuts."[4] According to an unclassified finding of the Defense Cyber Crime Center (DC3), "Cold Cuts" was also present on the computer network of Anthem, though another intrusion set has been attributed to the exfiltration of PII from Anthem. "Cold Cuts" used a particular technique of registering "doppelganger" domains to aid its activity. According to DC3:

> "Cold Cuts" registers domain names that are very similar to legitimate domain names of organizations they intend to or have targeted via computer network exploitation. These domains are referred to as "doppelganger" domains. Through in-depth analysis of domain registrant data, DC3 has identified approximately 70 doppelganger domain names likely indicative of a potential target for Cold Cuts operations.[5]

Companies targeted by Cold Cuts included OPM, Anthem and other companies, some of which hold government contracts.

II. ATTACKERS EXPLOITED TRUSTED CONTRACTOR/AGENCY RELATIONSHIP TO OBTAIN SENSITIVE INFORMATION ABOUT U.S. PERSONNEL

A. Attackers In The 2015 OPM Data Breach Mimicked A Contractor Employee's Network Credentials To Get Past OPM's Defenses

Mr. Wagner explained that the attackers in the 2015 OPM data breach mimicked the network credentials of an individual working for KeyPoint Government Solutions, a contractor that had been retained by the Federal Investigative Services (FIS). KeyPoint performs background investigations used in determining suitability for security clearances. Mr. Wagner explained:

> They came in as a KeyPoint FIS contractor. They had looked like a KeyPoint FIS contractor. They acted like a KeyPoint FIS contractor. And once in the environment,

---

[3] House Committee on Oversight and Government Reform, Transcribed Interview of Jeff Wagner, Director of Security Operations, Office of Personnel Management (Feb. 18, 2016).

[4] Defense Cyber Crime Command, *(U//FOUO) Cold Cuts Doppelganger Domain Analysis* (DC3-AG-Special Report 15-003) (Mar. 19, 2015).

[5] *Id.*

they transformed into either a domain administrator or they utilized a domain administration account.[6]

Brendan Saulsbury, the OPM contract employee who detected the second breach, explained that the intruders used the privileged access that KeyPoint network accounts require as part of the process of transmitting background investigation information gathered by KeyPoint investigators:

> So the Federal investigative systems background investigator contractors when—they will [connect via a Virtual Private Network] VPN into OPM's network in order to access the [Personnel Investigations Processing] PIP system to upload their background investigations. So what we saw was a machine coming from that VPN connection that was maliciously accessing these infected systems.[7]

B. Attackers Exploited Contractor Access to Data to Obtain PII of Federal Employees

Contracting companies that were victims of the sophisticated campaign maintained databases of sensitive information about federal employees.

For instance, in August 2014, USIS, a contractor that conducted background checks for OPM, reported that its networks had been breached, and, as a result, the personal information of thousands of federal employees had been compromised.[8]

KeyPoint reported that it was breached in a 2014 cyber-attack. According to OPM, this breach may have resulted in the theft of PII of approximately 48,000 employees.[9]

Anthem insures millions of federal workers. The January 2015 breach of its network exposed the PII of over two million federal employees to attackers.[10]

---

[6] House Committee on Oversight and Government Reform, Transcribed Interview of Jeff Wagner, Director of Security Operations, Office of Personnel Management (Feb. 18, 2016).

[7] House Committee on Oversight and Government Reform, Transcribed Interview of Brendan Saulsbury, Senior Cybersecurity Engineer, SRA International (Feb. 17, 2016).

[8] *DHS Contractor Suffers Major Computer Breach, Officials Say*, Washington Post (Aug. 6, 2014) (online at www.washingtonpost.com/world/national-security/dhs-contractor-suffers-major-computer-breach-officials-say/2014/08/06/8ed131b4-1d89-11e4-ae54-0cfe1f974f8a_story.html).

[9] *KeyPoint Network Breach Could Affect Thousands of Federal Workers*, Washington Post (Dec. 18, 2014) (online at 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).

[10] Briefing from Anthem to House Committee on Oversight and Government Reform Staff (May 17, 2016).

Mr. Wagner summarized the campaign's effect on the security of sensitive information about federal employees this way:

> The same timeframe, same time periods, OPM as well as its direct subcontracts were all systematically targeted, breached, and had adversarial activity in which data was lost, all related to specific data associated with those entities. Health insurance companies lost PII associated with annuitants—or not annuitants—but insurers, while FIS contractors lost PII data that was within their entities. OPM didn't store, necessarily data to FIS contractor sites; however, those contractors were contracted to perform background investigations for other Federal entities, and any data that was stored for those entities was lost.[11]

Determination of the intended purpose of the adversary was beyond the scope of the Committee's investigation. However, non-governmental cyber security professionals suspected espionage:

> It is possible that the adversary's goal for these compromises was to build a dataset on a large number of individuals of intelligence value through which detailed profiles of these individuals could be produced. Such a project would require the theft of PII from multiple organizations such as those observed in this campaign.[12]

III. TOP CYBER OFFICIALS BELIEVED OPM FREE OF MALWARE MONTHS BEFORE 2015 BREACH

A. Following Detection of Data Breach in 2014, Interagency Team Directed OPM's Malware Clean-up and Security Enhancing Upgrade

The interagency team, consisting of law enforcement and intelligence community agencies, advised OPM how to eject the network intruders. According to Mr. Wagner:

> In our discussions with DHS and others, they felt it was best to do a "Big Bang" remediation or essentially, do everything all at once. So we utilized the holiday weekend as a method to pre-stage everything so we could initiate as big of a change as possible to try to just throw the adversary out.

He added:

> [W]e implemented additional [Tactics, Techniques and Procedures] indicators into our systems; we installed additional connectors and taps and other pieces as well. But these steps here were the biggest steps to remove the adversarial presence and change all

---

[11] House Committee on Oversight and Government Reform, Transcribed Interview of Jeff Wagner, Director of Security Operations, Office of Personnel Management (Feb. 18, 2016).

[12] CrowdStrike, *2015 Global Threat Report* (2016) (online at http://go.crowdstrike.com/rs/281-OBQ-266/images/15GlobalThreatReport.pdf).

account passwords. … So when we did a full [Active Directory] credential change, we changed everything.[13]

The interagency team recommended nine steps to eradicate the adversary. These steps included removing all known compromised systems from the network, password changes, deployment of additional sensors, and additional audit logs.

B. Interagency Team Scanned Network for Weeks and Monitored for Malicious Activity, But Found None

After the "Big Bang" remediation, cyber experts from DHS and the Intelligence Community believed they had ejected the intruders. Their scans of the network and their monitoring efforts supported this belief. When asked to explain the results of these scans and monitoring, Mr. Wagner had this exchange with Committee staff:

Q: After 5/27, did you conduct scans, aggressive scanning of the network, to ensure that the "Big Bang" had removed all the attackers' foothold?

A: Yes. We conducted multiple scans. DHS remained with their Mandiant tool for another 30 or 45 days. We even had regular checkups with US-CERT, where I'd go over to the Glebe address and talk to them to see if there was any communication throughout DHS, FBI the IC community, if anything was being identified related to OPM, and there was no communication whatsoever.[14]

Mr. Wagner also had this exchange with Committee staff:

Q: So after you completed the remediation plan, on a scale of one to ten, how confident would you say you were that you had removed the attackers' foothold from OPM's environment?

A: The entire interagency team felt that it was fairly confident that there was no evidence of adversarial activity.

Q: Sounds like a ten?

A: IT guys are never 100 percent, so I'll give you 9.5.[15]

On June 22, 2014, DHS certified the following: "No new systems communicating with known C2 servers; no new attacker activity observed."[16]

---

[13] House Committee on Oversight and Government Reform, Transcribed Interview of Jeff Wagner, Director of Security Operations, Office of Personnel Management (Feb. 18, 2016).

[14] *Id.*

[15] *Id.*

[16] Department of Homeland Security, *OPM Incident Report* (June 22, 2014).

IV. CLAIMS THAT A PRIVATE COMPANY CONDUCTING A PRODUCT DEMONSTRATION HAD DISCOVERED THE OPM BREACH ARE FALSE

In response to an inquiry from the House Permanent Select Committee on Intelligence in June 2015, the Committee also investigated claims made by a private company in the *Wall Street Journal* that it had been the first entity to detect the cyber intrusion of 2015.

> Four people familiar with the investigation said the breach was actually discovered during a mid-April sales demonstration at OPM by a Virginia company called CyTech Services, which has a networks forensics platform called CyFIR. CyTech, trying to show OPM how its cybersecurity product worked, ran a diagnostics study on OPM's network and discovered malware was embedded on the network. Investigators believe the hackers had been in the network for a year or more.[17]

House Republicans repeated these claims. For instance, Rep. Michael Turner asked OPM Director Archuleta and Ms. Seymour at an Oversight Committee hearing: "Was CyTech involved in the discovery of this data breach?" In response, Ms. Seymour explained that "OPM discovered the breach." With respect to CyTech's subsequent scan, she explained: "We wanted to see if that tool set would also discover what we had already discovered." Rep. Turner then replied:

> Well, clearly, you are going to have to give us all an additional briefing and certainly the Intel Committee staff an additional briefing on exactly how you did this because, you know, CyTech's relating what they did is very compelling. And, quite frankly, what you say sounds highly suspicious, that you would have brought them in, tricked them to see if they could discover it, something you have already discovered.[18]

Contrary to these claims, the evidence obtained by the Committee indicates that OPM discovered the breach on April 15 or 16, 2015—five or six days before CyTech conducted its product demonstration and its scan of OPM's systems.

As part of our investigation, the Committee obtained a report issued by the United States Computer Emergency Readiness Team (US-CERT) on April 24, 2015, stating that OPM discovered suspicious activity on its networks on April 16, 2015. On that date, OPM "requested that US-CERT conduct digital media analysis of three server images/hard drives." The report states that between April 16 and 20, 2015, "OPM also provided US-CERT with a document containing information on suspicious IP Addresses and domains that may have been involved with the incident."[19]

---

[17] *U.S. Spy Agencies Join Probe of Personnel-Records Theft: Sales Demonstration May Have Uncovered Government Breach*, Wall Street Journal (June 10, 2015).

[18] House Committee on Oversight and Government Reform, *Hearing on OPM Data Breach: Part II* (June 24, 2015).

[19] United States Computer Emergency Readiness Team, *Preliminary Digital Media Analysis Report (PDMAR) No. INC 465355* (Apr. 24, 2015).

The Committee also obtained a follow-on report issued by US-CERT on June 9, 2015, stating that on April 15, 2015, OPM discovered an unknown Secure Sockets Layer (SSL) certificate on its network that was being used to encrypt communications with the known malicious domain "opmsecurity.org."[20] The encrypted communications were detected and successfully analyzed because of hardware and procedures implemented under the guidance of OPM CIO Donna Seymour as part of the agency's enhanced security measures.[21]

Brendan Saulsbury, the OPM contract engineer who actually detected the unknown SSL certificate as part of his work in OPM's Security Operations Center (SOC), told the Committee how OPM first became aware of the breaches:

> Q: Who specifically within OPM, SOC first detected the malicious activity that was behind the April 2015 cyber intrusion?
>
> A: Myself.
>
> Q: And was it on April 16, 2015, that you recall detecting the malicious activity?
>
> A: I believe so.
>
> Q: Can you tell us what specifically was the malicious activity you detected on OPM's network on April 16, 2015?
>
> A: We observed malware beaconing out to a command and control server from, at the time, two different servers.[22]

Mr. Saulsbury also explained that the malware he detected was disguised as McAfee antivirus files:

> [W]e were able to determine that the actual malware was a DLL file that was called mcutil.dll. It was basically trying to fly under the radar as if it was a McAfee antivirus executable. The problem is that OPM doesn't use McAfee, so that stood out right there to us that, at that point, I was 100 percent certain that this is malware that is beaconing out.[23]

---

[20] United States Computer Emergency Readiness Team, *Digital Media Analysis Report (DMAR) No. 465355* (June 9, 2015).

[21] Letter from Jason K. Levine, Director, Congressional, Legislative and Intergovernmental Affairs, Office of Personnel Management, to Chairman Jason Chaffetz and Ranking Member Elijah E. Cummings, House Committee on Oversight and Government Reform (Sept. 25, 2015).

[22] House Committee on Oversight and Government Reform, Transcribed Interview of Brendan Saulsbury, Senior Cybersecurity Engineer, SRA International (Feb. 17, 2016).

[23] *Id.*

On February 18, 2016, Committee staff conducted a transcribed interview with Jeff Wagner, OPM's Director of Security Operations, who confirmed Mr. Saulsbury's account. Mr. Wagner had this exchange with Committee staff:

> Q: Earlier you mentioned that on April 15, 2015, OPM recognized an unknown certificate attached to a sophisticated attacker. So how did you first come to learn on April 15, 2015, that OPM's network may have been compromised?
>
> A: My first indication was in the discussion of an unknown certificate through email.
>
> ...
>
> Q: So we're clear, was it folks working in OPM's Security Operations Center, or SOC, that first detected malicious activity on OPM's network?
>
> A: Yes.
>
> Q: And do you recall any of the names of folks within the SOC who were responsible for first detecting the malicious activity on April 15, 2015?
>
> A: Jon Tonda, my lead engineer, would have been doing log investigation, and Brendan Saulsbury would have been the one pulling the forensics logs and doing the reverse engineering.[24]

Mr. Wagner also explained that the tool used to identify the malware was developed by a different contractor, Cylance, which Ms. Seymour had previously hired to enhance OPM's cybersecurity:

> Because of the unique capability of Cylance in mapping binary files as opposed to looking at direct signatures, we knew it was going to be able to immediately find any malware no matter what the indicators were.[25]

On April 17, 2015, Mr. Wagner sent an email to Ms. Seymour reporting that Cylance officials were "coming in to help with the forensics" because it was "their tool that found the Malware."[26] He sent this email five days before CyTech conducted its product demonstration.

On September 30, 2015, Committee staff conducted a transcribed interview of Ben Cotton, the President and CEO of CyTech, who stated: "I had discovered that they were not

---

[24] House Committee on Oversight and Government Reform, Transcribed Interview of Jeff Wagner, Director of Security Operations, Office of Personnel Management (Feb. 18, 2016).

[25] *Id.*

[26] Email from Jeff Wagner, Director of Security Operations, Office of Personnel Management, to Donna Seymour, Chief Information Officer, Office of Personnel Management (Apr. 17, 2015).

using McAfee as an anti-virus. But three of these processes were masquerading as McAfee executables."[27]

The evidence obtained by the Committee confirmed that the malware OPM identified was the same malware CyTech identified during its product demonstration a week later. As Mr. Saulsbury, explained, CyTech "didn't detect anything that we didn't already know about."[28]

More recently, CyTech has continued to make inaccurate assertions to defend its false claim of the malware's discovery. For instance, in an article in *NextGov*, Ben Cotton asserted that, "it is extremely rare that you would allow malware to continue to exist inside of your organization for a full week after you discovered it's there."[29]

Mr. Cotton's statement is inaccurate. The tactic of allowing an adversary to continue to access a compromised network is commonly employed to allow law enforcement and the Intelligence Community to study the adversary's tactics, techniques, and procedures to both get a better understanding of the source of the attacks, and to design countermeasures to future attacks.

In an exchange with Committee staff, Mr. Wagner explained how this standard protocol was used after the breaches at OPM:

> Q: So when OPM was monitoring the malicious activity in 2014, was it doing that monitoring under the advice and guidance of any governmental agency?
>
> A: Yes. So the 2014 incident, the interagency response team of OPM, DHS, FBI were all involved under the monitoring. So any changes to the activity would automatically notify those three agencies through a process or a procedure that was put in place. So if the adversary's activity was from 10 p.m. to 10 a.m. but it was normally in a period of 3 to 4 a.m. where they were active, when they would throw something on our network or send a script to the network, I would get a phone call. I would then call DHS and FBI. So it was a concerted effort. It wasn't simply OPM by itself.
>
> Q: And what's the basic goal of doing this monitoring activity?
>
> A: The biggest reason is because, with the advancement of adversarial activity and some of the advanced malware that's currently capable, it's to try to find all potential connections to the environment. Just because you have one known

---

[27] House Committee on Oversight and Government Reform, Transcribed Interview of Ben Cotton, President and CEO, CyTech Services (Sept. 30, 2015).

[28] House Committee on Oversight and Government Reform, Transcribed Interview of Brendan Saulsbury, Senior Cybersecurity Engineer, SRA International (Feb. 17, 2016).

[29] *The Puzzle of When the OPM Hack Was Discovered Might Not Be Solved After All*, NextGov (May 31, 2016) (online at www.nextgov.com/cybersecurity/2016/05/probe-when-opm-hack-was-discovered-might-not-be-case-closed/128698/).

> TTP or one piece of malware doesn't mean that there aren't additional pieces of malware installed or present.[30]

V. INADEQUATE CONTRACT REQUIREMENTS WEAKENED SECURITY FOR SENSITIVE INFORMATION ON U.S. PERSONNEL

A. Top Officials Faulted Inadequate Contract Requirements

In 2015, the Committee received testimony that one of the weak links in the government's cybersecurity chain was the prevalence of inadequate clauses in U.S. government contracts with private-sector companies. Federal CIO Tony Scott testified that the breaches at USIS and KeyPoint made clear that "Federal agencies did not have adequate contractual language, policy direction, or awareness of best practices to guide how contractors and agencies should respond to intrusions and/or actual breaches."[31]

At the same hearing, then-OPM CIO Donna Seymour testified on what the cyber-attacks against OPM and its contractors revealed about the need for improvements in the agency's contract clauses: "We learned there were significant differences in our ability to understand and respond to these attacks because of the way sensitive information is exchanged, because of technical architecture, and because of the contractual relationship with the company."[32]

Ms. Seymour also testified as to the types of clauses that had been missing from OPM's contracts with vendors:

> Clauses that require segregation of data. One of the lessons that we learned is that if you have a network where all the data is comingled, then it is very difficult to protect the data, to segregate the data, understand what the adversaries are about and, therefore, protect that information. If the data is well architected and segregated, you have a better chance of understanding what the adversaries are after and putting better protections around it in a very quick manner.[33]

Ms. Seymour's testimony explained the connection between strong contract clauses and the security of sensitive government information: "When the government has a well-defined relationship with the contractor that specifically addresses information security and incident management, it is easier to work with the company to obtain information and plan remediation efforts."[34]

---

[30] House Committee on Oversight and Government Reform, Transcribed Interview of Jeff Wagner, Director of Security Operations, Office of Personnel Management (Feb. 18, 2016).

[31] House Committee on Oversight and Government Reform, *Hearing on Enhancing Cybersecurity of Third-Party Contractors and Vendors* (Apr. 22, 2015).

[32] *Id.*

[33] *Id.*

[34] *Id.*

B. After USIS Breach, Federal Cyber Officials Had To "Negotiate" With Company To Examine Compromised Network.

Following the data breach of USIS, the company that performed most of OPM's background investigations for federal employees, US-CERT did not have strong contractual access to USIS' computer networks to allow it to conduct a robust forensic analysis.

According to Donna Seymour:

> The Government was able to negotiate with USIS to allow US-CERT to scan their network and uncover some of the vulnerabilities and propose remediation steps for USIS. We were limited somewhat in our ability to scan the network, or US-CERT was limited in its ability to scan the network, again, because of the architecture of the USIS network, so US-CERT was given permission to scan two of the subnets of that network that they identified.[35]

When Ms. Seymour was asked whether federal cyber officials were "able to accomplish everything you wanted to accomplish with regard to USIS?" she responded: "We were not able to go to the boundaries of the network."

VI. SINCE BREACHES, FEDERAL OFFICIALS HAVE BEEN FOCUSING ON IMPROVING CONTRACT REQUIREMENTS

A. Steps Taken By OMB

In response to the data breaches at OPM, KeyPoint, and USIS, federal officials have sought to improve the government's cybersecurity through strengthening federal contracts.

On April 22, 2015, Federal CIO Tony Scott testified on the immediate steps OMB took to improve contract language in the wake of the breaches. He explained:

> OMB directed an inter-agency effort to collect and disseminate contracting best practices to help agencies ensure the protection of sensitive government information… The inter-agency effort to collect and disseminate contracting best practices included direction from OMB to the Federal CIO Council and Chief Acquisition Officers (CAO) Council to provide recommendations to OMB for next steps to bolster cyber protections in [f]ederal contracts.[36]

B. Steps Taken By OPM

OPM took action to improve contracting requirements with its vendors in response to the KeyPoint and USIS data breaches. On April 22, 2015, then-OPM CIO Seymour testified that in response to those breaches, the agency had taken two steps: "One is we have reviewed our

---

[35] House Committee on Oversight and Government Reform, *Hearing on Enhancing Cybersecurity of Third-Party Contractors and Vendors* (Apr. 22, 2015).

[36] *Id.*

contract clauses to strengthen them, and the second thing that we are doing is we are reviewing all of our contracts to make sure that we have the appropriate clauses across the board in our OPM contracts."[37]

On May 12, 2016, the Committee received an update from OPM on the improvements the agency has made to its contracting clauses in response to questions submitted by Ranking Member Cummings after a hearing on security clearance reforms.[38] Acting OPM Director Beth Cobert reported that since undertaking a review of its contract clauses: "OPM has completed an update to the IT contract clauses in 2016 … to strengthen the reporting requirements by contractors in the event of a security breach."[39]

The 2016 contract clauses OPM had completed updates for were clauses that concerned the following: "The requirements for contractors to notify OPM of all IT security incidents, to whom the reports must be made, and when the report must be made as well as tighter timelines for reporting for future OPM IT contracts."[40]

Under the new 2016 contract clauses, contractors are now required to report any incident concerning information security to OPM "no later than 30 minutes after becoming aware of the [information security incident.]."[41]

The new 2016 contract clauses also expand OPM's right of access to any contractor IT system that involves a cybersecurity incident in which information security may have been compromised. Specifically, the clauses now provide that:

> During the period of performance of the contract and throughout any contract close-out period, the [c]ontractor must provide OPM, or its designate, with immediate access to all IT systems used by the [c]ontractor to support the performance of the contract for the purpose of inspection and forensic analysis in the event of an Information Security Incident (ISI).[42]

---

[37] *Id.*

[38] Email from Jennifer Tyree, Deputy Director, Office of Congressional and Legislative Intergovernmental Affairs, Office of Personnel Management, to Staff, House Committee on Oversight and Government Reform (May 12, 2016) (attaching Acting Director Beth Cobert's responses to additional questions Committee Members had submitted in connection with House Committee on Oversight and Government Reform, *Hearing on Security Clearance Reform: The Performance Accountability Council's Path Forward* (Feb. 25, 2016)).

[39] Letter from Beth Cobert, Acting Director, Office of Personnel Management, to Question for the Record by Ranking Member Cummings, House Committee on Oversight and Government Reform, *Hearing on Security Clearance Reform: The Performance Accountability Council's Path Forward* (Feb. 25, 2016).

[40] *Id.*

[41] *Id*, at Attachment 2.

[42] *Id.*

C. Steps Taken By DOD

Since the 2015 OPM data breach, the Department of Defense (DOD) has taken action to improve the contractual clauses it requires for contractors, which are set forth in the Defense Federal Acquisition Regulation Supplement (DFARS).

On March 31, 2016, the Committee received an update on the improvements DOD has made to its contracting clauses in response to questions Ranking Member Cummings submitted after the hearing on security clearance reforms.[43] DOD CIO Terry Halvorsen reported that in August and December 2015, DOD updated DFARS Clause 252.204-7012, to provide as follows:

> DFARS Clause 252.204-7012 was renamed "Safeguarding Covered Defense Information and Cyber Incident Reporting," and the scope of the clause was expanded to cover the safeguarding of covered defense information and require[s] contractors to report cyber incidents involving this new class of information as well as any cyber incident that may affect the ability to provide operationally critical support.[44]

The "covered defense information" in DFARS Clause 252.204-7012 now requires contractors to protect and report unclassified information that is either (1) "[p]rovided to the contractor by or on behalf of [DOD] in connection with the performance of the contract;" or (2) "used, or stored by or on behalf of the contractor in support of the performance of the contract" and falls into any of the following categories, controlled technical information, critical information, or export control.[45]

DOD CIO Halvorsen also reported that in addition to updating the clauses for safeguarding unclassified information, DOD also added a new clause that covered cloud computing services, "DFARS Clause 252.239-7010."[46] As he explained, this clause was added "to provide standard contract language for the acquisition of cloud computing services; including access, security and reporting requirements."[47]

---

[43] Email from Mark Mereand, Legislative Analyst, Department of Defense, to Staff, House Committee on Oversight and Government Reform (Mar. 31, 2016) (attaching Department of Defense Chief Information Officer Terry Halvorsen's responses to additional questions Committee Members submitted in connection with House Committee on Oversight and Government Reform, *Hearing on Security Clearance Reform: The Performance Accountability Council's Path Forward* (Feb. 25, 2016)).

[44] Letter from Terry Halvorsen, Chief Information Officer, Department of Defense, to Question for the Record, by Ranking Member Elijah E. Cummings, House Committee on Oversight and Government Reform, *Hearing on Security Clearance Reform: The Performance Accountability Council's Path Forward* (Feb. 25, 2016).

[45] DFARS Clause 252.204-7012.

[46] Letter from Terry Halvorsen, Chief Information Officer, Department of Defense, to Question for the Record by Ranking Member Elijah E. Cummings, House Committee on Oversight and Government Reform, *Hearing on Security Clearance Reform: The Performance Accountability Council's Path Forward* (Feb. 25, 2016).

[47] *Id.*

VII. IMPLEMENTATION OF NEW CONTRACT REQUIREMENTS NOT YET COMPLETED

A. OPM Requirements Under Development

OPM is completing work on new contract clauses that would improve the government's capability to access a contractor's IT systems in the event of a data breach.[48] These new contract clauses are intended to address the challenge the government faced in the Anthem data breach when the company "declined to let US-CERT investigate the breach."[49] Acting Director Cobert explained: "The new contract clauses ... expand OPM's ability to access contractors' IT systems to perform inspections and forensic analysis by US-CERT or any other agency involved in remediation in the event of a cyber breach."[50]

B. OMB Requirements Under Development

In August 2015, OMB first released for public comment and feedback proposed guidance for assisting federal agencies in implementing improved cybersecurity protections when contracting for goods or services. The public feedback period closed on September 10, 2015, and OMB is now in the process of finalizing this guidance.[51]

The guidance being finalized by OMB would "strengthen government agencies' clauses regarding the type of security controls that apply, notification requirements for when an incident occurs, and the requirements around assessments and monitoring of systems."[52] The new guidance will have the following characteristics:

1. Security Controls

Agencies that utilize contractors whose IT systems are "operated on behalf of the Government" must include contract clauses that "require the contractor system to meet the appropriate baseline in NIST [Special Publication] 800-53."[53] Special Publication 800-53 "provide[s] guidelines for selecting and specifying security controls for organizations ... supporting the executive agencies of the federal government." NIST Special Publication 800-53

---

[48] Letter from Beth Cobert, Acting Director, Office of Personnel Management, to Question for the Record by Ranking Member Elijah E. Cummings, House Committee on Oversight and Government Reform, *Hearing on Security Clearance Reform: The Performance Accountability Council's Path Forward* (Feb. 25, 2016).

[49] House Committee on Oversight and Government Reform, *Hearing on Security Clearance Reform: The Performance Accountability Council's Path Forward* (Feb. 25, 2016).

[50] *Id.*

[51] Office of Management and Budget, *Improving Cybersecurity Protections in Federal Acquisitions Public Comment Space* (online at www.policy.cio.gov) (accessed May 27, 2016).

[52] *Id.*

[53] *Id.*

was originally designed "to achieve more secure information systems and effective risk management within the federal government."[54]

By mandating that contract clauses include language requiring contractors to adhere to NIST Special Publication 800-53, contractors must now "conform to the same processes as do government systems."[55]

2. Cyber Incident Reporting

OMB found that "agency contracts often lack language governing when and how contractors are required to report information security incidents when they occur and when and how contractors should provide notification of breaches to affected individuals and third parties."[56]

The new guidance will require all agencies to include contract language that address in detail a contractor's obligation to report a cybersecurity incident to an agency. At a minimum, the type of language OMB specifies that agencies must include when addressing cybersecurity reporting in a contract, includes, among other things, the following:

- A definition of what constitutes a "cyber incident" for purpose of reporting. Under the guidance, a "cyber incident" refers to "actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein;"
- A required timeline for first reporting a cyber incident to an agency;
- The categories of information a contractor must report in a cyber incident, which, at a minimum, must include, the specific type of information compromised; and
- Specific remedies for the government should a contractor fail to report a cyber incident in accordance with the agreed upon contractual language.[57]

According to OMB, the incorporation of these clauses into agency contracts "will promote timely and meaningful information sharing that allows both the contractor and the agency to work closely together to investigate the incident, identify affected individuals, quickly respond to the incident, and take other appropriate actions as necessary."[58]

---

[54] National Institute of Standards and Technology, Special Publication 800-53 Revision 4, § 1.1.

[55] Office of Management and Budget, *Improving Cybersecurity Protections in Federal Acquisitions Public Comment Space* (online at www.policy.cio.gov) (accessed May 27, 2016).

[56] *Id.*

[57] *Id.*

[58] *Id.*

3. Information System Security Assessments

The guidance will also address the scope of contractual language that should be included "for assessing information systems that a contractor is operating on behalf of Federal agencies." Under the guidelines, contractual clauses should, among other things, specify the following: "[T]hat the contractor will afford the agency access to the contractor's facilities, installations, operations, documentation, databases, IT systems, devices, and personnel used in performance of the contract, regardless of location."[59]

4. Information Security Continuous Monitoring

The guidelines further address the challenge of "information security continuous monitoring" in government contracts. "Information security continuous monitoring" refers to the practice of "maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions."[60]

Under the guidelines, in the event an agency finds it would not be practicable to use tools that are provided by DHS for the continuous monitoring of a contractor-operated system, a contract must include language that at a minimum, provides: "The agency may elect to perform information security continuous monitoring and IT security scanning of contractor systems with tools and infrastructure of its choosing."[61]

VIII. EVIDENCE DOES NOT SUPPORT JUSTIFICATIONS USED BY CHAIRMAN CHAFFETZ FOR DEMANDING THE RESIGNATION OF OPM CIO

A. Chairman Called for CIO's Resignation Before Committee Started Investigation, Claiming Breach Was "Foreseeable"

Before the Committee began its investigation, Chairman Chaffetz claimed that the OPM data breach was "foreseeable," and he called for the resignation of then-CIO Donna Seymour on at least five occasions.

The first time was on June 24, 2015, during a Committee hearing on the OPM data breach. Two days later, he and 17 Republican members of the Committee wrote to President Barack Obama requesting removal of Ms. Seymour and OPM's then-Director, Katherine Archuleta, asserting, "The recent breach was entirely foreseeable."[62]

Following Ms. Archuleta's resignation, Chairman Chaffetz wrote to Acting Director Beth Cobert to urge her to remove Ms. Seymour. He wrote:

---

[59] *Id.*

[60] *Id.* (quoting National Institute of Standards and Technology, Special Publication 800-137).

[61] *Id.*

[62] Letter from Chairman Jason Chaffetz, House Committee on Oversight and Government Reform, to President Barack Obama (June 26, 2015).

Despite repeated warnings from the OPM Inspector General, Ms. Seymour failed to prevent breaches of personally-identifiable information, harming over 22 million federal employees and other individuals, and weakening our national security.[63]

In December, Chairman Chaffetz wrote again to Acting Director Cobert to accuse Ms. Seymour of being "unfit to perform the significant duties for which she is responsible."[64]

When Ms. Seymour resigned in February 2016, Chairman Chaffetz said: "On her watch, whether through negligence or incompetence, millions of Americans lost their privacy and personal data. The national security implications of this entirely foreseeable breach are far-reaching and long-lasting."[65]

B. Evidence Does Not Support Chairman's Rationale

1. 2014 Breach Began Before Seymour Was Hired

The 2014 OPM breach started before Donna Seymour was hired. Jeff Wagner had this exchange explaining the chronology of Seymour's hiring and the 2014 data breach:

Q: Is there anything Ms. Seymour, in your assessment, could have reasonably done to prevent the 2014 incident?

A: No.

Q: And with respect to the 2014 incident, the attackers were in before she ever started as CIO, correct?

A: Correct.

Q: Okay. And when were the attackers, with regard to the 2014 incident—the earliest OPM was able to determine was within its system?

A: So the earliest evidence of adversary activity that the interagency team was able to identify was November of 2013.

Q: And Ms. Seymour started as CIO in either December 2013 or January 2014 from your recollection, correct?

---

[63] Letter from Chairman Jason Chaffetz, House Committee on Oversight and Government Reform, to Acting Director Beth Cobert, Office of Personnel Management (Aug. 6, 2015).

[64] Letter from Chairman Jason Chaffetz, House Committee on Oversight and Government Reform, to Acting Director Beth Cobert, Office of Personnel Management (Dec. 10, 2015).

[65] Chairman Jason Chaffetz, House Committee on Oversight and Government Reform, *Chaffetz Responds to Retirement of OPM CIO Donna Seymour* (Feb. 22, 2016).

A: Correct.[66]

2. Intelligence Community Certified OPM Free of Intruder Activity in June 2014 Though Forensic Analysis Would Later Show Second Breach Already Underway

Following the first breach and OPM's remediation efforts, monitoring of adversarial activity by the Intelligence Community did not detect the existence of another data breach. On June 22, 2014, DHS certified the following: "No new systems communicating with known C2 servers; no new attacker activity observed."[67]

3. 2014 and 2015 Breaches Detected by Security Tools Donna Seymour Deployed

Ms. Seymour is credited with immediately improving overall cybersecurity. According to Mr. Wagner, "With the week she started as CIO, she met with the director and began drafting the 100-day CIO plan."[68]

Similarly, according to Brendan Saulsbury:

> Things got a lot better when Donna Seymour came on board. I think her coming from a DOD background sort of helped us. I want to say that—I mean, I can't speculate as to whether she understood the threat better, but it became easier for Jeff [Wagner] to accomplish his goals.[69]

Ms. Seymour's hiring marked the beginning of improvements in OPM's cyber defenses, including enhanced tools to scan the network for malicious activity.

According to DHS's OPM incident report for the 2014 breach, OPM detected the adversary only after implementation of new security enhancements to their monitoring capability. As the report makes clear: "It should be noted the attackers had access to OPM's network since July of 2012 and the documents … were exfiltrated during the time period of March 2014 to May 2014 when OPM CIRT started their advanced monitoring of the infected systems."[70]

Prior to Ms. Seymour's enhancements, OPM did not have the ability to detect the cyber attackers' exfiltration of documents from OPM. When asked to explain the state of OPM's cyber

---

[66] House Committee on Oversight and Government Reform, Transcribed Interview of Jeff Wagner, Director of Security Operations, Office of Personnel Management (Feb. 18, 2016).

[67] Department of Homeland Security, *OPM Incident Report* (June 22, 2014).

[68] *Id.*

[69] House Committee on Oversight and Government Reform, Transcribed Interview of Brendan Saulsbury, Senior Cybersecurity Engineer, SRA International (Feb. 17, 2016).

[70] Department of Homeland Security, *OPM Incident Report* (June 22, 2014).

detection capabilities before the enhancements made while Ms. Seymour was Director, Mr. Wagner had this exchange with Committee staff:

> Q: So prior to March 2014, is it fair to say that OPM would not have known if data had been exfiltrated?
>
> A: We did not know—we would not know exactly what was exfiltrated.[71]

Over the course of 2014 and into 2015, Ms. Seymour's cybersecurity enhancements continued to be deployed. Those enhancements enabled OPM to detect the second breach, even after the interagency team's scans had failed to detect it.

According to Mr. Saulsbury, the engineer credited with finding the malware in the 2015 breach, "I would say that it is unlikely that OPM would have been able to detect that incident without those tools being put in place." Mr. Saulsbury also had this exchange with Committee staff:

> Q: And earlier you mentioned that you had seen noticeable improvements with network security under Donna Seymour, does the OPM tactical toolset that has been marked exhibit 3 reflect those improvement as you look at it?
>
> A: Yes.[72]

Federal CIO Tony Scott also credited Ms. Seymour for implementing the enhancements that enabled OPM to detect the data breach: "It was because of Donna and her team's actions that OPM identified the cyber breach of its systems."[73]

C. Chairman's Approach in Unfairly Blaming CIO Likely to Impair Recruitment and Retention of Talented IT Professionals

The persistent and unjustified calls by Chairman Chaffetz for Ms. Seymour's removal had the unfortunate and detrimental effect of forcing out the key leader who was responsible for substantially improving OPM's cyber capabilities and detecting the breaches.[74] At a critical time in which OPM was in need of strong IT leadership, these actions deprived OPM of a CIO from

---

[71] House Committee on Oversight and Government Reform, Transcribed Interview of Jeff Wagner, Director of Security Operations, Office of Personnel Management (Feb. 18, 2016).

[72] House Committee on Oversight and Government Reform, Transcribed Interview of Brendan Saulsbury, Senior Cybersecurity Engineer, SRA International (Feb. 17, 2016).

[73] *Embattled OPM CIO Steps Down,* Federal Computer Weekly (Feb. 22, 2016) (online at https://fcw.com/articles/2016/02/22/donna-seymour-quits.aspx).

[74] *OPM CIO Seymour Resigns Days Before Oversight Hearing*, Federal Times (Feb. 22, 2016) (online at www.federaltimes.com/story/government/it/cio/2016/02/22/opm-cio-seymour-resigns/80766440/).

February 22, 2016, to August 9, 2016, when the agency announced it had hired Mr. David DeVries to serve as the agency's new CIO.[75]

Reflexively calling for the removal of federal CIOs any time sophisticated cyber actors compromise their respective agencies' networks will likely have a chilling effect on the government's ability to recruit and retain talented information technology professionals.

[75] Office of Personnel Management, *OPM Announces New Chief Information Officer: David De Vries Joins OPM After Distinguished Service as Principal Deputy CIO at DOD* (Aug. 9, 2016).