Committee on Oversight and Government Reform

U.S. House of Representatives

114th Congress

The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation

Majority Staff Report

Hon. Jason Chaffetz, Chairman
Committee on Oversight and Government Reform

Hon. Mark Meadows, Chairman
Subcommittee on Government Operations

Hon. Will Hurd, Chairman
Subcommittee on Information Technology

September 7, 2016

www.oversight.house.gov

A Letter from the Chairman

September 7, 2016

To Federal Chief Information Officers:

The advent of the information age presents a paradigm shift about how our federal institutions collect, store, distribute, and protect information. The data breach at the U.S. Office of Personnel Management (OPM) is a defining moment, and it is up to you—the community of federal chief information officers—to determine how the country will respond.

The effectiveness of our country's response depends on your answer to this question: Can you as the CIO be trusted with highly personal, highly sensitive data on millions of Americans? Federal CIOs possess expertise and technical knowledge that support the mission-related activities of their agency. As Departmental heads focus on managing the bureaucracy of the executive branch, substantive challenges of their agencies' mission, and Congress, CIOs play a critical role in keeping technology working for Americans, and in furtherance of the agencies' mission.

Federal CIOs matter. In fact, your work has never been more important, and the margin for error has never been smaller.

As we continue to confront the ongoing challenges of modernizing antiquated systems, CIOs must remain constantly vigilant to protect the information of hundreds of millions of Americans in an environment where a single vulnerability is all a sophisticated actor needs to steal information, identities, and profoundly damage our national security.

The mission of our Committee is to ensure the efficiency, effectiveness, and accountability of the federal government and its agencies. We have a constitutional duty to provide meaningful oversight of the executive branch and to recommend reforms that are informed by our investigative findings. Taxpayers also rely on the Committee to bring a measure of accountability and transparency in cases where there is evidence of misconduct.

That is why I am releasing this report to the American public. For those whose personal information was compromised, I hope this report provides some answers on the how and why. Most of all, however, it is my hope that the findings and recommendations contained herein will inform and motivate current and future CIOs and agency heads so we – as a government – can be smart about the way we acquire, deploy, maintain, and monitor our information technology. The OPM data breach and the resulting generational national security consequences cannot happen again. It is up leaders like you and Congress to ensure it does not happen again.

Sincerely,

Jason Chaffetz
Chairman

The Damage Done

"This is crown jewels material . . . a gold mine for a foreign intelligence service."

"This is not the end of American human intelligence, but it's a significant blow."[*]

— Joel Brenner, former NSA Senior Counsel

"We cannot undo this damage. What is done is done and it will take decades to fix."[†]

— John Schindler, former NSA officer

"[The SF-86] gives you any kind of information that might be a threat to [the employee's] security clearance."[‡]

— Jeff Neal, former DHS official

"My SF-86 lists every place I've ever lived since I was 18, every foreign travel I've ever taken, all of my family, their addresses. So it's not just my identity that's affected. I've got siblings. I've got five kids. All of that is in there."[§]

— James Comey, Director of the FBI

"[OPM data] remains a treasure trove of information that is available to the Chinese until the people represented by the information age off. There's no fixing it."[**]

— Michael Hayden, former Director of the CIA

---

[*] David Perera & Joseph Marks, *Newly Disclosed Hack Got "Crown Jewels,"* POLITICO, June 12, 2015, available at: http://www.politico.com/story/2015/06/hackers-federal-employees-security-background-checks-118954.

[†] *Ex-NSA Officer: OPM Hack is Serious Breach of Worker Trust*, NPR, June 13, 2015, available at: http://www.npr.org/2015/06/13/414149626/ex-nsa-officer-opm-hack-is-serious-breach-of-worker-trust.

[‡] Id.

[§] Maggie Ybarra, *James Comey, FBI Chief, Says His Own Info was Hacked in OPM Breach; It was "Enormous"*, WASH. TIMES, July 9, 2015, available at: http://www.washingtontimes.com/news/2015/jul/9/james-comey-fbi-chief-says-his-own-info-was-hacked.

[**] Dan Verton, *Impact of OPM Breach Could Last More Than 40 Years*, FEDSCOOP.COM, July 12, 2015, available at: http://fedscoop.com/opm-losses-a-40-year-problem-for-intelligence-community.

Executive Summary

The government of the United States of America has never before been more vulnerable to cyberattacks. No agency appears safe. In recent data breaches, hackers took information from the United States Postal Service; the State Department; the Nuclear Regulatory Commission; the Internal Revenue Service; and even the White House.

None of these data breaches though compare to the data breaches at the U.S. Office of Personnel Management (OPM). **In what appears to be a coordinated campaign to collect information on government employees, attackers exfiltrated personnel files of 4.2 million former and current government employees and security clearance background investigation information on 21.5 million individuals.**[1] Additionally, fingerprint data of 5.6 million of these individuals was stolen.

The loss of personally identifiable information (PII) is deeply troubling and citizens deserve greater protection from their government. Further, the damage done by the loss of the background investigation information and fingerprint data will harm counterintelligence efforts for at least a generation to come.

The Significance of What the Attackers Stole. Certain individuals apply for a security clearance to gain access to our country's most sensitive national security secrets. These individuals are required to complete Standard Form 86 or "SF-86" and undergo a background investigation. Many applicants are obvious targets by adversaries for intelligence purposes by virtue of their holding some of the most sensitive positions in our government, including anyone accessing classified information and anyone employed in a "national security sensitive position." This encompasses a wide-range of federal employees and contractors at all federal agencies, including the U.S. Department of Defense and throughout the Intelligence Community.

Background investigations conducted on these individuals are designed to identify the type of information that could be used to coerce an individual to betray their country. Therefore, applicants are required to provide a wealth of information about their past activities and lifestyle. For example, applicants are required to provide extensive financial information, as well as employment history and home addresses for the past ten years. Applicants are also required to provide the names of any relatives, including step-siblings or half-siblings, and their home addresses.

The SF-86 also requests disclosure of some of the most intimate and potentially embarrassing aspects of a person's life, including whether the applicant:

---

[1] There is some overlap between the 4.2 million individuals impacted by the personnel records breach and the 21.5 million individuals impacted by the background investigation breach. Of the 4.2 million individuals impacted by the personnel records breach, 3.6 million on these individuals also had their background investigation data stolen. *See* Letter from Jason Levine, Dir. Congressional, Legislative & Intergov't Affairs, U.S. Office of Personnel Mgmt. to Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform (Aug. 21, 2015). The aggregate number of individuals impacted by this breach totals 22.1 million.

- "consult[ed] with a health care professional regarding an emotional or mental health condition;"
- "illegally used any drugs or controlled substances;"
- abused alcohol resulting in "a negative impact on your work performance or personal relationships, your finances, or result in intervention by law enforcement/public safety personnel;" and
- "experienced financial problems due to gambling."

In short, the SF-86 asks individuals to turn over their most personal details; information that in the wrong hands could be used for espionage purposes.

The intelligence and counterintelligence value of the stolen background investigation information for a foreign nation cannot be overstated, nor will it ever be fully known. The Director of the Federal Bureau of Investigation (FBI) James Comey described the data breach as a "very big deal from a national security perspective and from a counterintelligence perspective. It's a treasure trove of information about everybody who has worked for, tried to work for, or works for the United States government."[2]

Nor is there any way to remedy the problem now that the information is in the hands of our adversaries. Former Central Intelligence Agency (CIA) Director Michael Hayden warned he does not "think there is recovery from what was lost" and "it remains a treasure trove of information that is available to the Chinese until the people represented by the information age off. There's no fixing it."[3]

How the Breach Happened. **Despite this high value information maintained by OPM, the agency failed to prioritize cybersecurity and adequately secure high value data**. The OPM Inspector General (IG) warned since at least 2005 that the information maintained by OPM was vulnerable to hackers. In 2014, the IG upgraded issues surrounding information security governance at OPM from a "material weakness" to a "significant deficiency." But fundamental aspects of OPM's information security posture, such as the absence of an effective managerial structure to implement reliable IT security policies, remained a "significant deficiency" or worse since 2007.[4] Indeed, even after the data breach as of November 2015, the OPM IG continued to report that "OPM continues to struggle to meet many FISMA requirements" and with "overall lack of compliance that seems to permeate the agency's IT security program."[5]

---

[2] Ellen Nakashima, *Hacks of OPM databases compromised 22.1 million people, federal authorities say*, WASH. POST, July 9, 2015, available at: https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/.

[3] Dan Verton, *Impact of OPM Breach Could Last More Than 40 Years*, FedScoop.com (July 12, 2015) available at: http://fedscoop.com/opm-losses-a-40-year-problem-for-intelligence-community.

[4] Office of Inspector Gen., U.S. Office of Pers. Mgmt, No. 4A-CI -00-14-016, *Federal Information Security Management Act Audit FY 2014* (Nov. 12, 2014) available at: https://www.opm.gov/our-inspector-general/reports/2014/federal-information-security-management-act-audit-fy-2014-4a-ci-00-14-016.pdf.

[5] Office of Inspector Gen., U.S. Office of Pers. Mgmt., No. 4A-CI-00-15-011, *Final Audit Report, Federal Information Security Modernization Act Audit FY 2015* 5 (Nov. 10, 2015) available at: https://www.opm.gov/our-inspector-general/reports/2015/federal-information-security-modernization-act-audit-fy-2015-final-audit-report-4a-ci-00-15-011.pdf [hereinafter *FY15 FISMA Audit*].

The agency also failed to implement the Office of Management and Budget's (OMB) longstanding requirement to use multi-factor authentication for employees and contractors who log on to the network. In a 2015 OMB report on IT security, OPM was identified at the end of fiscal year 2014 as one of several agencies with the "weakest authentication profile[s]" and only having one percent of user accounts requiring personal identity verification (PIV) cards for access.[6] The agency also allowed key IT systems, which were later compromised, to operate without a security assessment and valid Authority to Operate (ATO). In 2014, the IG called the increasing number of OPM IT systems operating without a valid ATO "alarming."[7]

The lax state of OPM's information security left the agency's information systems exposed for any experienced hacker to infiltrate and compromise. On March 20, 2014, the U.S. Department of Homeland Security's (DHS) United States Computer Emergency Response Team (US-CERT) notified OPM's Computer Incident Response Team (CIRT) that a third party had reported data exfiltration from OPM's network. In an effort to better understand the threat posed by the hacker, OPM monitored the adversary's movements over a two-month period. **The agency's senior leadership failed to fully comprehend the extent of the compromise, allowing the hackers to remove manuals and other sensitive materials that essentially provided a roadmap to the OPM IT environment and key users for potential compromise.**

While OPM monitored the first hacker (for convenience here we will refer to this actor as Hacker X1), on May 7, 2014 another hacker posed as an employee of an OPM contractor performing background investigations, KeyPoint (which we can call Hacker X2). Hacker X2 used the contractor's OPM credentials to log into the OPM system, install malware, and create a backdoor to the network.

As the agency monitored Hacker X1's movements throughout the network, it noticed Hacker X1 was getting dangerously close to the security clearance background information. OPM, in conjunction with DHS, developed a plan to kick Hacker X1 out of the system. It termed this remediation "the Big Bang." The agency was confident the planned remediation effort in late May 2014 eliminated Hacker X1's foothold on their systems. But Hacker X2, who had successfully established a foothold on OPM's systems and had not been detected due to gaps in OPM's IT security posture, remained in OPM's system post-Big Bang.

The Exfiltration of the Security Clearance Files Could Have Been Prevented. After the May 27 Big Bang, Hacker X2 moved around OPM's system until they began exfiltrating data in July 2014. As OPM's Director of IT Security Operations Jeff Wagner explained, the KeyPoint credential was used for the initial attack vector and then the attacker used various tactics to obtain domain administrator credentials to ultimately perform operations and maintain persistence from malware. Beginning in July through August 2014, the Hacker X2 exfiltrated the security clearance background investigation files. Then in December 2014, personnel records were exfiltrated, and in early 2015, fingerprint data was exfiltrated.

---

[6] Office of Mgmt. & Budget, Exec. Office of the President, *FY 2014 Annual Report to Congress: Federal Information Security Management Act* at 23, 20 (Feb. 27, 2015) available at: https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy14_fisma_report_02_27_2015.pdf.

[7] U.S. Office of Personnel Mgmt. Office of the Inspector General, *Federal Information Security Management Act Audit FY 2014* at 9 (Nov. 12, 2014) available at: https://www.opm.gov/our-inspector-general/reports/2014/federal-information-security-management-act-audit-fy-2014-4a-ci-00-14-016.pdf.

Had OPM implemented basic, required security controls and more expeditiously deployed cutting edge security tools when they first learned hackers were targeting such sensitive data, they could have significantly delayed, potentially prevented, or significantly mitigated the theft. Testimony from DHS made clear OPM's implementation of two-factor authentication for remote logons in early 2015, which had long been required of federal agencies, would have "precluded continued access by the intruder into the OPM network." Further, if OPM had fully deployed in a preventative mode available security tools and had sufficient visibility to fully monitor their network in the summer of 2014, they might have detected and stopped Hacker X2 before they had a chance to exfiltrate the security clearance background investigation files. **Importantly, the damage also could have been mitigated if the security of the sensitive data in OPM's critical IT systems had been prioritized and secured.**

The exact details on how and when the attackers (X1, X2) gained entry and established a persistent presence in OPM's network are not entirely clear. This is in large part due to sloppy cyber hygiene and inadequate security technologies that left OPM with reduced visibility into the traffic on its systems.

The data breach by Hacker X1 in 2014 should have sounded a high level multi-agency national security alarm that a sophisticated, persistent actor was seeking to access OPM's highest-value data. It was not until April 15, 2015 that OPM identified the first indicator its systems were compromised by Hacker X2. From April 16, 2015 through May 2015 (during the primary incident response period), security tools from an outside contractor, Cylance Inc., consistently detected key malicious code and other threats to OPM. While these types of security tools were generally available to OPM, the agency did not choose to deploy a preventative technology until *after* the agency was severely compromised and until *after* the agency's most sensitive information was lost to nefarious actors.

Notably, OPM's Director of IT Security Operations, Jeff Wagner, recommended deploying Cylance's preventative technology to insulate OPM's enterprise from additional attacks after the initial attack by Hacker X1 in March 2014. The Committee obtained documents and testimony proving OPM's information security posture was undermined by a woefully unsecure IT environment, internal politics and bureaucracy, and misplaced priorities related to the deployment of security tools that slowed vital security decisions. **Swifter action by OPM to harden the defenses of its IT architecture could have prevented or mitigated the damage that OPM's systems incurred.**

While OPM continued its incident response efforts throughout April 2015, another outside contractor named CyTech Services, provided forensic support after conducting an onsite demonstration of its technology "CyFIR." While OPM and CyTech provide differing accounts of the role of CyFIR in detecting unknown malware on OPM's systems, it is clear CyTech detected malware and assisted for at least two week in the response to the 2015 data breaches. To date, CyTech has not been compensated for any of its work. The Anti-Deficiency Act (ADA) prohibits a federal agency from accepting voluntary services without payment and without obtaining an agreement in writing that the contractor will never seek payment. In this case, there was no such agreement. Most concerning, the agency destroyed 11,035 files and directories located on CyTech's device prior to returning the device to its owner while a request from the

Committee for this information was pending. All of those files were material to the Committee's investigation, responsive to the Committee's subpoena requests for information and documents, and subject to a preservation order by the Committee.

OPM Misled Congress and the Public to Diminish the Damage. As the agency assessed the damage caused by the hackers, OPM downplayed the fallout. **OPM failed to proactively announce the 2014 breach to the public, and claimed the two cyberattacks were not connected. The 2014 and 2015 incidents, however, appear to be connected and possibly coordinated**. The first confirmed adversarial activity for both incidents came within a two-month span in November and December 2013. The hack discovered in March 2014 by Hacker X1 appeared to move through the system looking for security clearance background investigation data and was removed when they got too close. Hacker X1 did, however, exfiltrate OPM's manuals and other sensitive materials, which would be useful for targeting background information data systems. Hacker X1 was cleared from the system in May 2014 during the Big Bang exercise. Within three months, Hacker X2 finished targeting and stealing OPM's background investigations data (by early August 2014). Hacker X2 later stole personnel records (in December 2014) and fingerprint data (in March 2015). **The two attackers shared the same target, conducted their attacks in a similarly sophisticated manner, and struck with similar timing.** Further, the manuals exfiltrated by Hacker X1 likely aided Hacker X2 in navigating the OPM environment.

The Committee's year-long investigation to understand *how* the attackers perpetrated their intrusion, movements, and ultimately the exfiltration of data began with hearings, wherein then-OPM Chief Information Officer (CIO) Donna Seymour made a series of false and misleading statements under oath regarding the agency's response to the incidents announced in 2015. Seymour testified that OPM purchased CyTech licenses, but OPM did not make any purchases from CyTech. She also testified that CyTech's CyFIR tool was installed in a quarantine environment for the demonstration, but this tool was running on a live environment at OPM when it identified malware on April 22, 2015.

Seymour also misled the public about the significance of the data stolen in the 2014 attack. She testified on April 22, 2015 that "our antiquated technologies may have helped us a little bit."[8] Two months later, on June 24, 2015, she testified that the stolen manuals that were a roadmap to OPM's systems were merely "outdated security documents."[9]

The Bottom Line. The longstanding failure of OPM's leadership to implement basic cyber hygiene, such as maintaining current authorities to operate and employing strong multi-factor authentication, despite years of warnings from the Inspector General, represents a failure of culture and leadership, not technology. As OPM discovered in April 2015, tools were available that could have prevented the breaches, but OPM failed to leverage those tools to mitigate the agency's extensive vulnerabilities.

---

[8] *Enhancing Cybersecurity of Third-Party Contractors and Vendors: Hearing Before the H. Comm. on Oversight & Gov't. Reform,* 114th Cong. (Apr. 22, 2015) [hereinafter *Enhancing Cybersecurity Hearing*] (statement of Donna Seymour, Chief Info. Officer of the U.S. Office of Pers. Mgmt.).

[9] *OPM Data Breach: Part II: Hearing Before the H. Comm. on Oversight & Gov't Reform*, 114th Cong. 69 (June 24, 2015) (hereinafter *Hearing on OPM Data Breach: Part II*) (statement of Donna Seymour, Chief Info. Officer of the U.S. Office of Pers. Mgmt.).

As a result, tens of millions of federal employees and their families paid the price. Indeed, the damage done to the Intelligence Community will never be truly known. Due to the data breach at OPM, adversaries are in possession of some of the most intimate and embarrassing details of the lives of individuals who our country trusts to protect our national security and its secrets.

This report documents how the government allowed this unthinkable event to happen and makes recommendations in an attempt to ensure this never happens again.

The Committee remains hopeful that OPM, under the new leadership of Acting Director Beth Cobert, is in the process of remedying decades of mismanagement.

Table of Contents

A Letter from the Chairman ii

The Damage Done iii

Executive Summary v

Table of Contents 1

Timeline of Key Events 5

Findings 14

Recommendations 20

Table of Names 28

Chapter 1: OPM's IT Security Record Preceding Breaches 30

- The Rise of Advanced Persistent Threat Hacking 30
- Federal Contractors Holding Sensitive Federal Employee Information Targeted and Attacked 31
- Federal Initiatives to Increase Information Security in Response to Increasing Attacks 34
- OPM Failed to Recognize the Threat and Implement Effective IT Security Measures When It Mattered 35
  - OPM's Cybersecurity Spending Consistently Trailed Other Federal Agencies 36
  - OPM Attempts to Balance IT Security with Competing Priorities 37
  - The Katherine Archuleta and Donna Seymour Era 42
- OPM Failed to Prioritize the Security of Key Data and Systems 47

Chapter 2: The First Alarm Bell – Attackers Discovered in 2014 Target Background Information Data and Exfiltrate System-Related Data 51

- Discovery & Incident Response for Attackers Discovered in 2014 52
- Monitoring the Adversary and the May 2014 "Big Bang" to Expel Attackers Discovered in 2014 55
- During the 2014 Incident Response Period the Exfiltration of PIPS-related Information Made Clear the Attackers' Target was Background Investigation Data Held in PIPS 62
- Tactics Techniques & Procedures (TTPs) of Attackers Discovered in 2014: Hikit Malware and SMB Protocol 67
- OPM's Network Logging Capabilities Limited Investigating the "How" and "How Long" for Attackers Discovered in 2014 71

Chapter 3: OPM Attempts to Mitigate the Security Gaps Identified in 2014 While Iron Man and Captain America Go to Work (May 2014 – April 2015) 75

- OPM's IT Security Posture and Mitigation Efforts After the May 2014 "Big Bang" 75
- Key 2014 US-CERT Recommendations Highlighted OPM IT Security Vulnerabilities 77
- OPM Efforts to Buy Security Tools to Secure the Legacy Network and Rebuild OPM's "Very Insecure, Insecurely Architected Network" 79
- OPM Missed Key Developments 81
- In April 2015, OPM Realized They Were Under Attack – Again 83

Captain America: The First Indicator that Led to the 2015 Discovery of the Background Investigation Data Breach 84
The Avengers: Anatomy of the Data Breach Discovered in 2015 85
Chapter 4: The Role of Cylance Inc. 91
OPM's "Cyber Climate" During Cylance Product Demonstrations 91
Overview of the Cylance Cyber Tools 93
April 15-16, 2015: The First 24 Hours 94
April 17, 2015: US-CERT Confirms PlugX 98
April 17, 2015: CylanceProtect Deployed 100
April 18, 2015: Protect Lights Up Like a Christmas Tree 102
April 19, 2015: Severity of the Situation Becomes Clear 103
April 20-23, 2015 – More Key Trojans Identified; OIG First Notified. 108
April 24-25, 2015 – OPM Upgrades Protect to Auto-Quarantine Mode. 110
April 26 – April 30, 2015: First Signs of Lost Background Materials 113
The Decision to Purchase CylanceProtect 116
Political Challenges on the Desktop 116
Counterpoint – Lack of FedRAMP Compliance 119
OPM Purchases Protect After Nearly Losing Access to It 121
Chapter 5: The CyTech Story 125
CyTech Is a Small Business Contractor with Significant Cyber Tool Capabilities 126
CyTech Was Invited to Conduct a Demo at OPM 127
Prior to the April 21, 2015 CyFIR Demonstration at OPM 128
The April 21, 2015 – April 22, 2015 CyFIR Demonstration at OPM 128
The CyTech Demo Turned into Incident Response and Forensic Support 135
CyTech Provided Onsite Incident Response and Forensic Support From April 23 to May 1, 2015 135
CyFIR Was Deployed on the OPM Network beginning in April 2015 and Remained on OPM's Network through August 2015 138
The *Wall Street Journal* Reports on CyTech's Role in the OPM Incident on June 10, 2015 141
CyTech Coordinated with OPM Prior to the June 10, 2015 Story 142
OPM and CyTech Respond to the Article 143
OPM Description of CyTech's Role Was Misleading 146
Archuleta and Seymour Provided Misleading Testimony to Committee 146
Data on CyTech's CyFIR Appliance Collected During the 2015 Incident Response Period was Deleted 148
OPM Retained CyTech's CyFIR Appliance Through August 2015 149
Before Returning the CyFIR Appliance OPM Deleted Key Data. 149
OPM "Sanitized" the CyFIR Appliance 151
OPM Violated the Anti-Deficiency Act 152
The ADA's prohibition on accepting voluntary services 152
The "gratuitous" services exception 152

The "emergencies" exception 153
The ADA applied to the OPM and CyTech Situation 153
CyTech expected to be paid 154
Chapter 6: Connections Between the 2014 and 2015 Intrusions 157
One Group, Several Names 158
The 2014 Data Breach: The Unique Malware of the Axiom Group 159
Malware Discovered during the 2015 Data Breach 162
2014 & 2015: Likely Connected, Possibly Coordinated 168
Chapter 7: OPM's OCIO and its Federal Watchdog 173
The IG's Memorandum of Concern 174
Four Instances Where the OCIO Failed to Cooperate Fully 177
Seymour failed to appropriately notify the IG of the April 2015 intrusion detection 177
Seymour failed to notify the OIG of the loss of background investigation data in a timely manner 180
Seymour failed to notify the OIG about the 2014 incident 182
Meetings with Federal Law Enforcement Agencies 183
KeyPoint Audit 184
Notification Concerning New IT Infrastructure 185
Five Incorrect and/or Misleading Statements 187
First Misstatement before the Senate Committee on Appropriations 187
Second Misstatement Before the Senate Committee on Appropriations 188
Third Misstatement Before Senate Committee on Appropriations and House Committee on Oversight and Government Reform 188
Fourth Misstatement Before the House Committee on Oversight and Government Reform 189
Fifth Misstatement Before the Senate 189
Current State of Relationship 189
Summary of OIG and OCIO relationship 193
Chapter 8: The IT Infrastructure Improvement Project: Key Weaknesses in OPM's Contracting Approach 194
The IG Issues a Flash Audit Alert and Interim Reports on the IT Infrastructure Project 196
The IG's Concerns Continued through the Fall of 2015 198
IG Reports Progress in Responding to Concerns, but Challenges Remain as of May 2016 198
The Story of OPM's IT Infrastructure Improvement Project and the Sole Source Contract 200
Timeline: OPM's IT Infrastructure Improvement Project 201
OPM Initiates Contact with Imperatis and Awards Sole Source Contract 205
Imperatis and OPM Buy Security Tools to Secure the Legacy IT Environment 206
Imperatis' Role in Responding to OPM Data Breach Incidents 207
Sole Source, Schedule, and Cost IG Concerns Related to OPM's IT Infrastructure Improvement Contract Validated 208
Summary of Investigation 214

Committee hearings on the data breaches 214
Committee request for information regarding identity theft services 215
Productions related to the OPM data breaches and CyTech 216
The Committee investigated the role of Cylance 219
The Committee investigated the role of SRA 220
The Committee Investigated OPM's IT Infrastructure Improvement Project and the Contract Awardee Imperatis 221
Document productions by Department of Homeland Security 221
Unnecessary delays, restrictions, redactions and a congressional subpoena 222
Unnecessary delays 222
Unnecessary redactions 222
Subpoena issued to OPM 224
Conclusion 225
Appendix: Cyber security Spending at OPM (Fiscal Years 2012-2015) 227

Timeline of Key Events

July 2012

- ✓ Attackers had access to OPM's network, according to US-CERT.[1] US-CERT found malware (Hikit) resided on an OPM server since 2012.[2]

November 2013

- ✓ First evidence of adversarial activity by the attacker associated with the breach that US-CERT informed OPM about in March 2014.[3]

December 2013

- ✓ First evidence of adversarial activity associated with the 2015 breaches (including harvesting of credentials from OPM contractors) by the attacker that was not identified until April 2015.[4]

March 20, 2014

- ✓ US-CERT notifies OPM of a data exfiltration from OPM's network.[5] OPM, working with US-CERT, determines and implements a strategy to monitor the attackers' movements to gather counterintelligence. This breach involved data that included manuals and IT system architecture information, but the full extent of exfiltrated data is unknown.

- ✓ The strategy remains in place until the "Big Bang" on May 27, 2014.

March 25, 2014

- ✓ Situation report takes place with CIO Donna Seymour and US-CERT.[6]

March 27, 2014

- ✓ As OPM monitors the hackers, it develops a "Plan for full shut down [of systems] if needed."[7]

---

[1] June 2014 OPM Incident Report at HOGR0818-001235 (OPM Production: Sept. 18, 2015) [hereinafter June 2014 OPM Incident Report]. Note: This Report was authored by DHS/US-CERT and provided to OPM.
[2] U.S. Dep't of Homeland Security/US-CERT, Digital Media Analysis Report-465355 (June 9, 2015) at HOGR0724-001154 (US-CERT Production: Dec. 22, 2015) [Hereinafter June 9, 2015 DMAR].
[3] *Hearing on OPM Data Breach: Part II* (statement of Donna Seymour, Chief Info. Officer of the U.S. Office of Personnel Mgmt.).
[4] Briefing by US-CERT to H. Comm. on Oversight & Gov't Reform Staff (Feb. 19, 2016).
[5] June 2014 OPM Incident Report at HOGR0818-001240.
[6] *Id.*
[7] *Id.*

April 11, 2014

- ✓ Tactical mitigation strategies and security remediation plan developed for briefing to Donna Seymour.[8]

April 21, 2014

- ✓ OPM contractor (SRA) discovers a "specific piece of malware," which is brought to US-CERT's attention.[9]

April 25, 2014

- ✓ "opmsecurity.org" is registered to Steve Rogers, a.k.a. "Captain America."[10] The hackers later used this domain for command and control (C2) and data exfiltration.[11]

May 7, 2014

- ✓ The attacker later associated with exfiltrating background investigation data establishes their foothold into OPM's network. This attacker poses as a background investigations contractor employee (KeyPoint), uses an OPM credential, remotely accesses OPM's network, and installs PlugX malware to create a backdoor.[12]

- ✓ OPM did not identify the attacker's May 7 foothold despite the fact that OPM was monitoring and removing another attacker (that US-CERT had notified OPM about in March 2014).

May 27, 2014

- ✓ OPM shuts down its compromised systems in the "Big Bang" event in an effort to remove the attacker. This decision was made after OPM observed the attacker "load a key logger onto . . . several database administrators' workstations" and they got

---

[8] *Id.* at HOGR0818-001241.
[9] *Id.* at HOGR0818-001242.
[10] ThreatConnect Research Team, *OPM Breach Analysis*, THREATCONNECT (June 5, 2015), available at: https://www.threatconnect.com/opm-breach-analysis/; H. Comm. on Oversight and Gov't Reform, Transcribed Interview of Brendan Saulsbury, Senior Cyber Security Engineer, SRA, Ex. 4 (Feb. 17, 2016) [Hereinafter Saulsbury Tr.].
[11] Briefing by US-CERT to H. Comm. on Oversight & Gov't Reform Staff (Feb. 19, 2016); Saulsbury Tr. at 59.
[12] H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Jeff P. Wagner, U.S. Office of Personnel Mmgt., Dir. of Information Technology Operations at 127-128 (Feb. 18, 2016) [hereinafter Wagner Tr.; Dep't of Homeland Sec./US-CERT and Office of Pers. Mgmt., OPM Cybersecurity Events Timeline (Aug. 26, 2015), at HOGR020316-000760-UR-A (OPM Production: May 13, 2016) [hereinafter OPM Cybersecurity Events Timeline]; Briefing by US-CERT to H. Comm. on Oversight & Gov't Reform Staff (Feb. 19, 2016). KeyPoint CEO testified that "there was an individual who had an OPM account who was a KeyPoint employee and [] the credentials of that individual were compromised to gain access to OPM." *Hearing on OPM Data Breach: Part II* (statement of Eric Hess, Chief Exec. Officer, KeyPoint). The OPM Director of IT Security Operations [Wagner] explained that "a KeyPoint user credential [was] utilized for [the] initial vector infection," but that "user did not have administrative credentials, so the adversary utilized tactics in order to gain domain administrator credentials" to move through the environment and conduct operations-related activities. Wagner Tr. at 86.

"too close to getting access to the PIPs system," which held the background investigation data.[13]

- ✓ Meanwhile, the attacker that established a foothold on May 7, 2014 continues their presence on the OPM network.

June 5, 2014

- ✓ Malware is successfully installed on a KeyPoint web server; accounts differ as to whether or not administrator privileges were used to install this malware.[14]

June 10, 2014

- ✓ OPM CIO Donna Seymour testifies before the Senate Homeland Security and Governmental Affairs' Subcommittee on OPM's *Strategic Information Technology Plan* and does not disclose at this hearing the "manuals" breach discovered in March 2014.[15]

June 12, 2014

- ✓ OPM executes a Cylance product evaluation agreement that allowed it to test the functionality of both Cylance products (V and Protect) for a limited period of time.[16]

June 20, 2014

- ✓ Attackers conduct a remote desktop protocol (RDP) session, indicating contact with "important and sensitive servers supporting . . . background investigation processes." The remote session was not discovered until spring 2015.[17]

June 22, 2014

- ✓ DHS issues a final incident report for the OPM "manuals" breach first discovered on March 20, 2014.[18]

---

[13] Saulsbury Tr. at 25-26.

[14] Briefing by US-CERT to H. Comm. on Oversight & Gov't Reform Staff (Feb. 19, 2016); Letter from KeyPoint Government Solutions to the Hon. Elijah E. Cummings, Ranking Member, H. Comm. on Oversight & Gov't Reform (July 2, 2015). Note: KeyPoint maintains that "No unaccounted security tokens were used during the time the malware was operational on KeyPoint's network." The US-CERT Report of the KeyPoint intrusion disagrees stating that "a domain administrator account was used to install the malware on the web server. US-CERT reported that this "administrator account" had "full access privileges."

[15] *A More Efficient and Effective Government: Examining Federal IT Initiatives and the IT Workforce: Hearing Before the S. Subcomm. on the Efficiency and Effectiveness of Fed. Programs & the Fed. Workforce of the S. Comm. on Homeland Sec. & Gov't Affairs*, 113th Cong. (June 10, 2014).

[16] H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Stuart McClure, Chief Exec. Officer, President & Founder, Cylance, Inc., Ex. 2 (Feb. 4, 2016) [hereinafter McClure Tr.].

[17] H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Chris Coulter, Managing Dir. of Incident Response and Forensics (Feb. 12, 2016), Ex. 18 [hereinafter Coulter Tr.]

[18] June 2014 OPM Incident Report at HOGR0818-001233-46.

June 23, 2014

- ✓ US-CERT/OPM identifies this as first known adversarial access to OPM's mainframe.[19]

July – August 2014

- ✓ Attackers successfully exfiltrate the background investigation data from OPM's systems.[20]

July 9, 2014

- ✓ OPM acknowledges the March 2014 "manuals" breach to the *New York Times*.[21] This information had not previously been disclosed publicly.

- ✓ OPM states that no PII was lost in the breach and does not disclose the exfiltration of the manuals.

July 29, 2014

- ✓ "opmlearning.org" is registered to Tony Stark, a.k.a. "Iron Man."[22] The attackers used this domain for command and control during their intrusion into OPM's environment.

August 16, 2014

- ✓ The malware installed on KeyPoint systems on June 5, 2014 ceased operational capabilities.[23]

October 2014

- ✓ FBI Cyber Division issues a Cyber Flash Alert regarding "a group of Chinese Government affiliated cyber actors who routinely steal high value information from US commercial and government networks through cyber espionage" and notes

---

[19] Dep't of Homeland Sec./US-CERT Briefing to Staff (Feb. 19, 2016); OPM Cybersecurity Events Timeline.
[20] Id.
[21] Michael S. Schmidt, David E. Sanger & Nicole Perlroth, *Chinese Hackers Pursue Key Data on U.S. Workers*, N.Y. TIMES, July 9, 2014, available at: http://www.nytimes.com/2014/07/10/world/asia/chinese-hackers-pursue-key-data-on-us-workers.html?hp&action=click&pgtype=Homepage&version=LedeSum&module=first-column-region&region=top-news&WT.nav=top-news&_r=2.
[22] ThreatConnect, *OPM Breach Analysis*; Saulsbury Tr., Ex. 4.
[23] Letter from KeyPoint Government Solutions to the Hon. Elijah E. Cummings, Ranking Member, H. Comm. on Oversight & Gov't Reform (July 2, 2015) (citing US-CERT Report (Aug. 30, 2014)). KeyPoint notes that "significantly, the malware was a "zero day" attack—it had an electronic signature that was not known by anti-virus/anti-malware software at that time."

activity associated with this group "should be considered an indication of a compromise requiring extensive mitigation…."[24]

- ✓ Meanwhile, the attackers move through the OPM environment to the U.S. Department of Interior (DOI) data center where OPM personnel records are stored.[25]

November 2014

- ✓ A group of private-industry security companies warns about threats to the human resources components of federal government and releases a report on Chinese Advanced Persistent Threat (APT) activity.[26]

December 2014

- ✓ 4.2 million personnel records are exfiltrated after attackers moved around OPM's system and through the DOI's database, which holds OPM personnel records.[27]

March 3, 2015

- ✓ "wdc-news-post[.]com" is registered by attackers. Attackers would use this domain for C2 and data exfiltration in the final stage of the intrusion.[28]

March 9, 2015

- ✓ The last beaconing activity to the unknown domain "opmsecurity.org" occurs. This domain was registered in April 2014 to Steve Rogers, a.k.a. "Captain America."[29]

March 26, 2015

- ✓ Fingerprint data appears to have been exfiltrated on or around this date.[30]

---

[24] Cyber Div., Fed. Bureau of Investigation, A-000042-MW, *FBI Cyber Flash Alert* (Oct. 15, 2014), http://www.slideshare.net/ragebeast/infragard-hikitflash.

[25] OPM Cybersecurity Events Timeline.

[26] Novetta, *Operation SMN: Axiom Threat Actor Group Report* 9 (2014), http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf (The report emphasizes "Hikit" malware, stating, "Among the industries we observed targeted or potentially infected by Hikit [included] Asian and Western government agencies responsible for [a variety of services such as] Personnel Management.").

[27] Briefing by US-CERT to H. Comm. on Oversight & Gov't Reform Staff (Feb. 19, 2016); OPM Cybersecurity Events Timeline.

[28] DOMAIN > WDC-NEWS-POST.COM, THREATCROWD.ORG (last visited June 28, 2016), available at: https://www.threatcrowd.org/domain.php?domain=wdc-news-post.com .

[29] Saulsbury Tr. at 59.

[30] June 9, 2015 DMAR at HOGR0724-001158; *see also* Dep't of Homeland Sec./US-CERT Briefing to Staff (Feb. 19, 2016); OPM Cybersecurity Events Timeline.

April 15, 2015

- ✓ After being alerted by an OPM contractor (SRA) working on IT security, OPM notifies US-CERT about suspicious network traffic related to opmsecurity.org.[31] This domain was registered to Steve Rogers, a.k.a. "Captain America" in April 2014 and the last beaconing activity occurred in March 2015.

April 16, 2015

- ✓ OPM contacts Cylance for technical support on use of Cylance V, which was an endpoint detection tool that OPM had purchased in September 2014.[32] Cylance V is not intended to be an enterprise-wide prevention tool.[33]

April 17, 2015

- ✓ OPM begins to deploy enterprise-wide (on a demonstration basis and in "Alert" mode) a Cylance tool called CylanceProtect. At this time CylanceProtect was not in quarantine mode, but the tool would later identify and alert OPM to the widespread presence of malware on their system. OPM brings Cylance onsite for incident response.[34] OPM does not upgrade this tool to the highest preventative setting.[35]

April 18-19, 2015

- ✓ CylanceProtect is deployed to over 2,000 devices as of this date, makes "tons of findings," and as a Cylance engineer described the tool, it "lit up like a Christmas tree" indicating widespread malicious activities within the OPM system.[36]

April 21, 2015

- ✓ CyTech Services arrives onsite to conduct a product demonstration with their CyTech Forensics and Incident Response (CyFIR) tool, and remains onsite until May 1, 2015 to assist with incident response.[37]

April 22, 2015

- ✓ Then-CIO Donna Seymour testifies before the Committee about cybersecurity and publicly discussed the discovery of the "manuals" breach saying, "the adversaries in today's environment are typically used to more modern technologies, and so in this case, potentially, our antiquated technologies may have helped us a little bit. But I

---

[31] June 9, 2015 DMAR at HOGR0724-001158.
[32] Coulter Tr., Ex. 1, 2.
[33] McClure Tr. at 8.
[34] McClure Tr. at 21-22.
[35] *Id.* OPM upgraded from the *Cylance V* tool to the *Cylance PROTECT* tool. However, the tool remains in "Alert" mode only, not "Quarantine mode."
[36] McClure Tr., Ex. 8; Coulter Tr. at 20-21.
[37] H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Benjamin Cotton, CyTech Services, Chief Executive Officer at 14-15 (Sept. 30, 2015) [hereinafter Cotton Tr.].

think also it comes down to culture and leadership, and one of the things that we were able to do at OPM was to recognize the problem."[38]

- ✓ OPM's Office of the Inspector General (OIG) learns of the breach for the first time after a staffer bumped into the OPM Director of Security Operations in the hallway.

- ✓ The staffer testified that OPM's Director of IT Security Operations said there was "no need" to notify the public of the breach.[39]

April 23, 2015

- ✓ OPM determines there had been a "major incident" involving the exfiltration of personnel records, which triggers a requirement to notify Congress.[40]

- ✓ OPM notifies Congress of a "major incident" on April 30, 2015.[41]

April 24, 2015

- ✓ OPM orders a global quarantine to address malware identified by CylanceProtect.[42]

April 26, 2015

- ✓ Cylance engineers identify adversarial activity related to an RDP session to a background investigation database indicating this session took place in June 2014.[43]

May 8, 2015

- ✓ US-CERT establishes with a high degree of certainty that personnel records data/PII had been stolen.[44]

May 20, 2015

- ✓ OPM determines there was a major incident regarding the exfiltration of background investigation data, which triggers a requirement to notify Congress.

- ✓ OPM notifies Congress on May 27, 2015.[45]

---

[38] *Enhancing Cybersecurity of Third-Party Contractors and Vendors: Hearing Before the H. Comm. on Oversight & Gov't. Reform,* 114th Cong. (Apr. 22, 2015) (statement of Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt.) (testifying that OPM was hacked and that no PII was taken). The word "manuals" is not used at this time, though it is how we have since described the 2014 breach.

[39] H. Comm. on Oversight & Gov't Reform, Transcribed Interview of U.S. Office of Pers. Mgmt. Office of Inspector Gen. Special Agent at 17-18 (Oct. 6, 2015) [hereinafter Special Agent Tr.].

[40] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073, 3080 (2014).

[41] OPM Cybersecurity Events Timeline.

[42] Coulter Tr., Ex. 16.

[43] Coulter Tr., Ex. 18.

[44] Briefing by US-CERT to H. Comm. on Oversight & Gov't Reform Staff (Feb. 19, 2016); OPM Cybersecurity Events Timeline.

- ✓ OPM indicates to the OIG that background investigation information may also be compromised.[46]

June 4, 2015

- ✓ OPM briefs the media and releases a press statement that revealed the personnel records of 4.2 million former and current federal employees have been compromised.[47]

June 8, 2015

- ✓ US-CERT establishes with a high degree of certainty that background investigation data/PII has been exfiltrated and stolen.[48]

June 16, 2015

- ✓ Then-OPM Director Katherine Archuleta acknowledges that background investigation data may be compromised.[49]

June 24, 2015

- ✓ Then-CIO Donna Seymour testifies before the Committee and minimizes the importance of data removed in 2014 "Manuals" breach, saying "those documents were some outdated security documents about our systems and some manuals about our systems."[50]

June 29, 2015

- ✓ The American Federation of Government Employees (AFGE) files a class action suit against OPM.[51]

---

[45] Briefing by US-CERT to H. Comm. on Oversight & Gov't Reform Staff (Feb. 19, 2016); OPM Cybersecurity Events Timeline.
[46] Special Agent Tr. at 46.
[47] U.S. Office of Pers. Mgmt., Press Release, *OPM to Notify Employees of Cybersecurity Incident* (June 4, 2015), https://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident/.
[48] Briefing by US-CERT to H. Comm. on Oversight & Gov't Reform Staff (Feb. 19, 2016); OPM Cybersecurity Events Timeline.
[49] *OPM: Data Breach: Hearing Before the H. Comm. on Oversight & Gov't Reform,* 114th Cong. (June 16, 2015) (statement of Katherine Archuleta, Dir., U.S. Office of Pers. Mgmt.).
[50] *Hearing on OPM Data Breach: Part II* (statement of Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt.).
[51] *American Federation of Government Employees v. U.S. Office of Pers. Mgmt.*, No. 1:15-cv-1015 (D.D.C. filed June 29, 2015).

June 30, 2015

- ✓ After 74 days of deployment to over 10,250 devices, CylanceProtect detected and blocked almost 2,000 pieces of malware (including critical samples related to the breach)—nearly one piece of malware for every five devices.

July 9, 2015

- ✓ OPM issues a press release confirming background investigation data for 21.5 million individuals was compromised.[52]

July 10, 2015

- ✓ OPM Director Katherine Archuleta resigns.

July 21, 2015

- ✓ The Committee sends the first of a series of document requests to OPM.

August 20, 2015

- ✓ OPM returns the CyFIR tool to CyTech with key information deleted. The CyFIR tool, before it was deleted, contained images from OPM's incident response of more than 11,000 files and directories.

September 23, 2015

- ✓ OPM updates its original estimate that 1.1 million fingerprint records were compromised. The new estimate: 5.6 million.[53]

February 22, 2016

- ✓ Prior to testifying before the Committee, OPM CIO Donna Seymour resigns.

February 24, 2016

- ✓ Committee's planned hearing, "OPM Data Breach: Part III", is cancelled in the wake of OPM CIO Donna Seymour's resignation.[54]

---

[52] Press Release, U.S. Office of Pers. Mgmt., *OPM Announces Steps to Protect Federal Workers and Others From Cyber Threats* (July 9, 2015) available at: https://www.opm.gov/news/releases/2015/07/OPM-Announces-Steps-to-Protect-Federal-Workers-and-Others-From-Cyber-Threats/.

[53] Press Release, U.S. Office of Pers. Mgmt., *Statement by OPM Press Secretary Sam Schumach on Background Investigations Incident* (Sept. 23, 2015) available at: https://www.opm.gov/news/releases/2015/09/cyber-statement-923/.

[54] *OPM Data Breaches: Part III: Hearing Before H. Comm. on Oversight & Gov't Reform,* 114th Cong. (Feb. 24, 2016) (hearing cancelled).

Findings

Chapter 1: Findings Related OPM IT Security Record

OPM has long been plagued by a failure of management to prioritize information security in practice, and to retain leaders that are committed to information security over the long haul.

FINDING: OPM leadership failed to heed repeated recommendations from its Inspector General (IG). OPM has historically maintained a fragmented IT infrastructure, and still lacks a full, accurate inventory of all its major IT systems. As the IG noted in its FY2015 audit, "failure to maintain an accurate inventory undermines all attempts at securing OPM's information systems."

FINDING: Over the 2005-2015 timeframe, OPM failed to sufficiently respond to growing threats of sophisticated cyber attackers.

FINDING: OPM failed to prioritize resources for cyber security. In FY 2013, FY 2014 and FY 2015, OPM spent seven million each year on cybersecurity—spending that was consistently at the bottom relative to all other agencies that are required to report such expenditures to the Office of Management and Budget.

FINDING: Slow implementation of critical security requirements such as dual factor authentication is a true case of misplaced priorities.

FINDING: As early as 2005, OPM's IG issued a warning in a semiannual report that given the sensitive data OPM holds on former and current federal employees and family members, any attack or breakdown "could compromise efficiency and effectiveness and ultimately increase the cost to the American taxpayer."

FINDING: Key OPM systems, including the Personnel Investigations Processing System (PIPS), Enterprise Server Infrastructure (ESI), and the Local Area Network/Wide Area Network (LAN/WAN) were all operating on expired Authorities to Operate at the time of the data breach.

Chapter 2: Findings Related to the OPM Data Breach Discovered in 2014

In the spring of 2014 OPM suffered a data breach that resulted in the loss of documents relating to the most valuable databases on OPM's IT environment.

FINDING: Due to security gaps in OPM's network and a failure to adequately log network activity, the country will never know with complete certainty all of the documents that the attackers exfiltrated from OPM in connection with the breach discovered in March of 2014.

FINDING: The 2014 attackers used an uncommon toolkit designed for late-stage persistence and data exfiltration. The malware observed on OPM's systems in 2014 were two variants of Hikit malware, termed Hikit A and Hikit B.

FINDING: During an approximately two-month period, OPM watched the adversaries take sensitive data relating to high-valued targets on OPM's systems, including the server that holds background investigation materials, but was never able to determine how the adversary initially gained entry into their network.

FINDING: The documents taken by the 2014 attackers included information about OPM's systems that would have given an adversary an advantage in hacking the background investigation database and other sensitive systems in OPM's environment.

Chapter 3: OPM Attempts to Mitigate the Security Gaps Identified in 2014 While Iron Man and Captain America Go to Work (May 2014 – April 2015)

FINDING: In June 2014, US-CERT issued an incident report with 14 observations and recommendations to address the security gaps identified after the 2014 "manuals" breach. US-CERT deemed OPM's network very insecure, insecurely architected, and found OPM had a significant amount of legacy infrastructure.

FINDING: US-CERT also said there was a gap in information technology leadership across OPM as an agency and that it was not uncommon for existing security policies to be circumvented to execute business functions while exposing the entire agency to unnecessary risk.

FINDING: Had OPM leaders fully implemented basic, required security controls – including multi-factor authentication – when they first learned attackers were targeting background investigation data, they could have significantly delayed or mitigated the data breach of background information.

FINDING: In April 2015, an OPM contract employee identified a domain ("opmsecurity.org") that was purposely named to emulate a legitimate looking website and upon further investigation found the domain had a randomized email address and was registered to Steve Rogers, a.k.a. "Captain America." This was one of the first indicators of compromise identified by OPM in April 2015.

Chapter 4: Findings Related to the Role of Cylance Inc.

Information security tools of Cylance Inc. detected critical malicious code and other threats to OPM in April 2015 and thereafter played a critical role in responding to the data breaches in 2015.

FINDING: While Cylance tools were available to OPM as early as June 2014, OPM did not deploy its preventative technology until April 2015 after the agency was severely compromised and the nation's most sensitive information was lost. Swifter action by OPM to deploy CylanceProtect would have prevented or mitigated the damage that OPM's systems incurred.

FINDING: Following the May 27, 2014 "Big Bang" remediation, OPM decided not to purchase and deploy CylanceProtect due to, as Cylance CEO Stuart McClure put it, "political challenges on the desktop," meaning overcoming the tensions between IT security and program functionality.

FINDING: On April 15, 2015, OPM found an indicator of compromise and turned to Cylance for assistance. Cylance tools immediately found the most critical samples of malicious code present at OPM related to the breaches and that correspond to findings of DHS US-CERT.

FINDING: As of April 18-19, 2015, CylanceProtect was deployed (in Alert mode) to over 2,000 devices, made "tons of findings," and as a Cylance engineer described the tool it "lit up like a Christmas tree" – indicating widespread malicious activities in OPM's IT environment.

FINDING: OPM's former Director, Katherine Archuleta and former CIO Donna Seymour made questionable statements under oath about OPM's use of a quarantine to isolate malware and malicious process during the incident response.

FINDING: OPM eventually purchased CylanceProtect on June 30, 2015, but only as it was about to lose access to the product (as the demonstration period was ending). Despite Cylance's proven value during the 2015 incident response, OPM failed to timely make payments.

Chapter 5: Findings Related to the Role of CyTech Services

On June 10, 2015, the Wall Street Journal (WSJ) reported that CyTech Services, Inc. network forensics platform "CyFIR" actually discovered that data breach at OPM in mid-April during a sales demonstration.

FINDING: CyTech, a service disabled veteran-owned small business contractor, did participate in several meetings with OPM in early 2015 to discuss the capabilities of their CyTech Forensics and Incident response (CyFIR) tool and provided a demonstration of their CyFIR tool on April 21, 2015 at OPM headquarters.

FINDING: During the April 21 demonstration CyTech did identify malware on the live OPM IT environment related to the incident. CyTech was not aware at the time that OPM had identified on April 15 an unknown Secure Sockets Layer (SSL) certificate beaconing to a malicious domain (opmsecurity.org) not associated with OPM.

FINDING: Beginning on April 22, 2015, CyTech offered and began providing significant incident response and forensic support to OPM related to the 2015 incident.

FINDING: CyTech did not leak information about their involvement with the OPM incident to the press.

FINDING: The testimony given by the (now former) OPM CIO, Donna Seymour, before the Committee on June 24, 2015 regarding the CyTech matter is inconsistent with the facts on the record.

FINDING: Documents and testimony show CyTech provided a service to OPM and OPM did not pay. The Anti-deficiency Act (ADA) prohibits a federal agency from accepting voluntary services.

Chapter 6: Findings Related to the Connections between the 2014 and 2015 Intrusions at OPM

The data breaches OPM suffered in 2014 and 2015 share commonalities relevant not only to attribution, but more importantly OPM's reaction or lack thereof in the wake of the 2014 intrusion.

FINDING: The data breach discovered in March 2014 was likely conducted by the Axiom Group. This conclusion is based on the presence of Hikit malware and other Tactics Techniques and Procedures (TTPs) associated with this group, which have been publicly reported.

FINDING: The data breaches discovered in April 2015 were likely perpetrated by the group Deep Panda (a.k.a. Shell_Crew, a.k.a. Deputy Dog) as part of a broader campaign that targeted federal workers. This conclusion is based on commonalities in the 2015 adversary's attack infrastructure and TTPs common to other hacks publicly

attributed to Deep Panda. These groups include Wellpoint/Anthem, VAE Inc., and United Airlines. However, the cyber intrusion and data theft announced by Anthem in 2015 is a separate attack by a separate threat actor group unrelated to the hack against OPM discovered in 2015.

FINDING: As publicly reported, both the Axiom and Deep Panda groups are highly likely to be state-sponsored threat-actor group supported by the same foreign government.

FINDING: It is highly likely that the 2014 and 2014/2015 cyber intrusions into OPM's networks were likely connected and possibly coordinated campaigns.

Chapter 7: Findings Related to the Relationship between the OPM OCIO and its IG

Federal watchdogs play a critical role in the federal government, partnering with agencies to improve and safeguard programs and operations, including during and after data breaches.

FINDING: The relationship between the OPM Office of the Inspector General (OIG) and Office of the Chief Information Officer (OCIO) became strained during the tenure of former Director Katherine Archuleta and former CIO Donna Seymour. The relationship became so strained that on July 22, 2015, then-Inspector General Patrick McFarland issued a memorandum to OPM's Acting Director Beth Cobert to share "serious concerns" regarding the OCIO.

FINDING: Former OPM Director Katherine Archuleta and former OPM CIO Donna Seymour engaged in activities that hindered the work of the OIG, including when:
(1) OPM's OCIO failed to timely notify the OIG of the 2014 and 2015 data breaches or the data that was compromised;
(2) Director Archuleta stated that the OIG could not attend certain meetings relating to the data breaches because the OIG's presence would "interfere" with the FBI and US-CERT's work;
(3) The OCIO failed to notify and involved OIG in a major IT investment to develop a new IT infrastructure; and
(4) The OIG delayed an audit of KeyPoint Government Solutions at the request of the OCIO after an October 16, 2014 meeting, only to learn later OPM knew in early September 2014 that KeyPoint had been breached and did not disclose this information to the OIG.

FINDING: Former OPM Director Katherine Archuleta and former OPM CIO Donna Seymour made five incorrect and/or misleading statements to Congress. These statements were:
(1) Director Archuleta testified June 23, 2015 before the Senate Committee on Appropriations, Subcommittee on Financial Services and General Government, that OPM completed a Major IT Business Case (formerly known as the OMB "Exhibit 300") for the infrastructure improvement project; contrary to the finding of the OPM OIG;

(2) At the same June 23, 2015 hearing, Director Archuleta testified that "my CIO has told me that we have, indeed, an inventory of systems and data," contrary to the findings of the OIG in both a flash audit alert and the FY 2014 FISMA audit;
(3) Director Archuleta and CIO Donna Seymour testified before the Senate Appropriations Committee and the House Committee on Oversight and Government Reform that the sole-source contract with OPM's contractor (Imperatis) for the IT Infrastructure Improvement project covered only the first two phases of this multiphase IT Infrastructure Improvement project, and contracts for the later phases (migration and cleanup) of the project had not been awarded. However, the OIG found that the sole-source contract provided for work under all four phases of the project;
(4) OPM CIO Seymour testified before the House Committee on Oversight and Government Reform on June 16, 2015 that the 11 OPM systems operating without authorization were no longer a concern because she had granted an interim authorization to these systems. However, the IG found that OMB does not allow interim or extended authorizations; and
(5) At a June 25, 2015 hearing held by the Senate Committee on Homeland Security and Governmental Affairs, Director Archuleta stated that OPM had received a special exemption from OMB related to system authorization because of the ongoing IT Infrastructure Improvement project; however, this claim could not be substantiated.

FINDING: The relationship between the OPM OIG and OPM leadership has improved under Acting Director Beth F. Cobert.

Chapter 8: Findings Related to the IT Infrastructure Improvement Project

In response to the data breach at OPM in 2014, and after identifying serious vulnerabilities in the OPM network, the agency, at the recommendation of DHS, initiated the IT Infrastructure Improvement project.

FINDING: OPM's IT Infrastructure Improvement project is a case study illustrating why agencies need to ensure robust communications with the OIG, particularly in responding to cybersecurity incidents. Former OPM CIO Seymour said she was not aware of a requirement "to notify the IG of every project that we take on."

FINDING: OPM's use of a sole-source contract in an emergency situation illustrates why there should be pre-established contract vehicles for cyber incident response and related services.

FINDING: There is a pressing need for federal agencies to modernize legacy IT in order to mitigate the cybersecurity threat inherent in unsupported, end of life IT systems and applications.

Recommendations

In 2015 OPM announced the largest data breach of personally identifiable information (PII) of 22.1 million Americans. This failure of culture and leadership cannot happen again. The federal government must recognize and mitigate the ever-increasing cyber threat and protect the information that Americans entrust to the government. While there was much that went wrong for years in the federal government's approach to information security, this episode presents an opportunity for Congress and other agencies to inject new leadership and a culture of security in federal IT. The recommendations listed below are aimed at taking lessons learned from the OPM experience and charting a path of ever vigilant IT security in order to secure the PII of Americans held by the federal government.

Recommendation 1 – Ensure Agency CIOs are Empowered, Accountable, and Competent

Each federal agency must ensure agency CIOs are empowered, accountable, competent and retained for more than the current average two year tenure. The CIO at federal agencies and independent executive agencies is a critical leader who should be accountable to the head of the agency. Under federal laws, such as the Federal Information Security Management Act (FISMA) and the Federal Information Technology Acquisition Reform Act (FITARA), CIOs are responsible for IT security and management functions within the agency. In the last two years, Congress revised FISMA and FITARA to reflect the new prioritization agency heads should place on IT management and security. CIOs typically serve an average of two years, but greater priority should be placed on retaining these leaders for at least five years.[55] This Committee, and in particular the IT subcommittee, has made IT management and security an oversight priority to ensure vigorous implementation of FISMA and FITARA. Such oversight has included a FITARA scorecard to assess agencies' implementation of this law. This oversight will continue and agencies will be expected to ensure there is an empowered, accountable, and competent CIO serving in this critical role.

Recommendation 2 – Reprioritize Federal Information Security Efforts Toward a Zero Trust Model

OMB should provide guidance to agencies to promote a zero trust IT security model. The OPM data breaches discovered in 2014 and 2015 illustrate the challenge of securing large, and therefore high-value, data repositories when defenses are geared toward perimeter defenses. In both cases the attackers compromised user credentials to gain initial network access, utilized tactics to elevate their privileges, and once inside the perimeter, were able to move throughout OPM's network, and ultimately accessed the "crown jewel" data held by OPM. The agency was unable to visualize and log network traffic which led to gaps in knowledge regarding how much data was actually exfiltrated by attackers.

To combat the advanced persistent threats seeking to compromise or exploit federal government IT networks, agencies should move toward a "zero trust" model of information security and IT

[55] Gov't Accountability Office, GAO-11-634, *Federal Chief Information Officers: Opportunities Exist to Improve Role in Information Technology Management* (Oct. 2011) (stating the average CIO's tenure is two years).

architecture. The zero trust model centers on the concept that users inside a network are no more trustworthy than users outside a network.[56] The zero trust model requires strictly enforced user controls to ensure limited access for all users and assumes that all traffic traveling over an organization's network is threat traffic until authorized by the IT team. In order to effectively implement a zero trust model, organizations must implement measures to visualize and log all network traffic, and implement and enforce strong access controls for federal employees and contractors who access government networks and applications.

Recommendation 3 – Reduce Use of SSNs by Federal Agencies

Federal agencies should reduce the use of Social Security Numbers (SSN) in order to mitigate the risk of identity theft. SSNs are key pieces of PII that can potentially be used to perpetrate identity theft. The potential for misuse of SSNs has raised questions about how the federal government obtains, uses, and protects the SSNs it obtains. In May 2007, OMB required all federal agencies to review their use of SSNs in agency systems and programs in order to identify opportunities to reduce such use.[57] Agencies were required to establish a plan, within 120 days of the memo, to eliminate the unnecessary collection and use of SSNs within 18 months. They were also required to participate in government-wide efforts to explore alternatives to the use of SSNs as a personal identifier for federal employees and in the administration of federal programs. In response to a 2016 request by Chairman Chaffetz, the U.S. General Accountability Office (GAO) is currently reviewing actions agencies have taken to reduce the use of SSNs government-wide, actions OMB has taken to ensure agencies have adhered to its directive, and what progress has been made in reducing the use of SSNs across the federal government. Congress should carefully monitor the progress of these important actions, and work with agencies to ensure steps are taken to efficiently and effectively reduce agency use of SSNs.

Recommendation 4 – Require Timely Justifications for Lapsed Authorities to Operate

Agencies that fail to re-authorize the authorities to operate (ATO) for their critical federal systems should be required to provide Congress, within 15 days of the system's authorization expiring, a justification as to why the system authorization was allowed to lapse. Designated critical information systems lacking adequate justification for a lapsed ATO should be removed immediately from the production environment.

ATOs provide a comprehensive assessment of the IT system's security controls and are a vital part of ensuring federal systems operate securely. FISMA requires agencies to assess the effectiveness of their information security controls, the frequency of which is based on risk but no less than annually. OMB Circular A-130, Appendix III required agencies to assess and authorize (formerly referred to as certify and accredit) their systems before placing them into operational environment and whenever there is a major change to the system, *but no less than*

---

[56] This model was proposed by Forrester Research Inc., an American-owned independent research and advisory firm. in response to a 2013 National Institute of Science and Technology (NIST) request for information entitled, "Developing a Framework to Improve Critical Infrastructure Cybersecurity" NIST RFI# 130208119-3119-01. *See* 78 Fed. Reg. 13024 (Feb. 26, 2013) available at: http://csrc.nist.gov/cyberframework/rfi_comments/040813_forrester_research.pdf.

[57] Memorandum from Office of Mgmt. & Budget, Exec. Office of the President, to the Heads of Exec. Dep'ts & Agencies, M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007) available at: https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf.

every three years thereafter.[58] At OPM, critical systems were operating in FY 2014 without a valid ATO.[59] Of the 21 OPM systems due for reauthorization in FY 2014, 11 were not completed on time and were operating without a valid authorization,[60] and several were among the most critical, containing the agency's most sensitive information.[61] This led the IG to warn OPM that "[t]he drastic increase in the number of systems operating without a valid Authorization is alarming, and represents a systemic issue of inadequate planning by OPM program offices to authorize the information systems that they own."[62] A failure to maintain current ATOs negatively impacts the security of federal information systems. As the OPM IG pointed out, "there are currently no consequences for OPM systems that do not have a valid Authorization to operate."[63]

Consequently, agencies should account for lapses to Congress and be prepared to take critical systems out of production. Further, at OPM, the IG recommended the adoption of administrative sanctions for the failure to meet security authorization requirements.[64] Congress and the Administration should consider options (including legislation or policy guidance) to ensure there are appropriate consequences for lapsed ATOs.

Recommendation 5 – Ensure Accountability and Empower DOD IT Officials Implementing Necessary Security Improvements for NBIB

Clear rules for accountability and dedicated funding should be established by the end of FY 2017 to ensure the U.S. Department of Defense (DOD) is successful in securing the background investigation materials that will now be held at the new National Background Investigations Bureau (NBIB). In an effort to reform the background investigation process and secure related data, this function will now reside at the new NBIB and the DOD CIO will be responsible for IT.[65] The DOD CIO has testified that he will ultimately answer to the Secretary of Defense in matters relating to NBIB and that DOD will provide short-term funding for IT at NBIB.[66]

---

[58] Office of Mgmt. & Budget, Exec. Office of the President, OMB Circular A-130, Management of Federal Information Resources (Nov. 28, 2000) available at: https://www.whitehouse.gov/omb/circulars_a130_a130trans4/. OMB Circular A-130 was recently updated and includes new guidance for agencies on Authorization to Operate and Continuous Monitoring. Office of Mgmt & Budget Exec. Office of the President, OMB Circular A-130 Management of Federal Information Resources (July 27, 2016) available at: https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf . The Committee expects to continue oversight in the areas covered by the revised A-130.

[59] Office of the Inspector Gen., U.S. Office of Pers. Mgmt., Report No. 4A-CI -00-14-016, *Federal Information Security Management Act Audit FY 2014* (Nov. 12, 2014) available at: https://www.opm.gov/our-inspector-general/reports/2014/federal-information-security-management-act-audit-fy-2014-4a-ci-00-14-016.pdf

[60] *Id.* at 9.

[61] E-mail from Inspector Gen. Staff, U.S. Office of Pers. Mgmt., to H. Comm. on Oversight & Gov't Reform Staff (Dec. 4, 2015) (on file with the Committee).

[62] Office of the Inspector Gen., U.S. Office of Pers. Mgmt., Report No. 4A-CI -00-14-016, *Federal Information Security Management Act Audit FY 2014*, at 9 (Nov. 12, 2014) available at: https://www.opm.gov/our-inspector-general/reports/2014/federal-information-security-management-act-audit-fy-2014-4a-ci-00-14-016.pdf.

[63] *Id.* at 10.

[64] *Id.* at 11.

[65] White House, Press Release, *The Way Forward for Federal Background Investigations* (Jan. 22, 2016), https://www.whitehouse.gov/blog/2016/01/22/way-forward-federal-background-investigations.

[66] *Security Clearance Reform: The Performance Accountability Council's Path Forward: Hearing Before the House Comm. on Oversight & Gov't Reform*, 114th Cong. (Feb. 25, 2016) (testimony of Terry Halvorsen, Chief Info. Officer, U.S. Dep't of Defense).

However, it is not yet clear whether future IT funding for NBIB will come from DOD, OPM, or another source.[67] It is also unclear how disagreements between DOD and OPM regarding IT security spending would be resolved.[68] To ensure that IT security is appropriately prioritized at NBIB, OPM and DOD should establish clear sources of funding and decision-making processes for IT security, and the OIG at both OPM and DOD should work to oversee such implementation and management.

Recommendation 6 – Eliminate Information Security Roadblocks Faced by Agencies

To the extent there are non-security related bureaucratic hurdles to quickly implementing IT security policies and deploying cyber tools, agencies should make every effort to streamline processes and prioritize security. The federal government's most important responsibility is to protect this nation and our citizens – including when it comes to protecting this nation against cyberattacks. The process of deploying security tools can be cumbersome and requires navigating a bureaucratic process that may involve notifying unions and overcoming program manager opposition.[69] Congress should enact legislation sponsored by Rep. Gary Palmer in the House (H.R. 4361) and Senator Joni Ernst (S. 2975) to clarify agencies' authority under FISMA by stating the heads of federal agencies are able to take timely action to secure their IT networks, and without being required to first provide unions with the opportunity to bargain.

Recommendation 7 – Strengthen Security of Federal Websites and Breach Notifications

Congress should enact H.R. 451, the Safe and Secure Federal Websites Act of 2015, legislation sponsored by Rep. Chuck Fleischmann that increases the certification requirements for public federal websites that process or contain PII. The bill requires an agency's CIO to certify the website for security and functionality prior to making it publicly accessible. The bill also increases the requirements for agencies when responding to an information security breach that involves PII. The events that unfolded at OPM in 2014 and 2015 demonstrated an unwillingness by some officials to notify the public of a PII compromise in a timely manner. The bill directs OMB to develop and oversee implementation of the certification requirements, which include reporting the breach to a federal cyber security center and notifying individuals affected by a PII compromise.

Recommendation 8 – Financial Education and Counseling Services Through Employee Assistance Programs

Congress should encourage federal agencies to provide federal employees with financial education and counseling services that are designed to help employees recognize, prevent and mitigate identity theft through existing Employee Assistance Programs (EAP). An EAP is a voluntary, work-based program that offers free and confidential assessments, short-term

---

[67] *Id.*

[68] *Id.*

[69] In the case of OPM's efforts to deploy a tool called Forescout (which is a tool to manage network access control for devices), there were deployment delays due in part to the need to notify unions. Imperatis Weekly Report (Aug. 3, 2015-Aug. 7, 2015), Attach. 6 at 000942 (Imperatis Production: Sept. 1, 2015) (stating "project sponsor is in notification stage with the Union" and mitigation was to "prepare updated project timeline, plan & memo to pilot ForeScout to non-union agency users.").

counseling, referrals, and follow-up services to employees who have personal and/or work-related problems.[70]

Recommendation 9 – Establish Government-wide Contracting Vehicle for Cyber Incident Response Services

OMB and the General Services Administration (GSA) should lead efforts to establish a government-wide contracting vehicle for Cyber Incident Response Services or Congress should establish a statutory requirement for such a vehicle. After the data breach discovered in March 2014, OPM awarded a sole source contract for a multi-phased IT Infrastructure Improvement project. Under this contract, OPM procured cybersecurity tools to secure their legacy IT environment. Instead of duplicative sole source contracts across various agencies, the federal government should have pre-established contracting vehicles that have the benefit of competition and are available to provide incident response services, including tools to secure IT environments post-breach.

Agencies should not be in the process of establishing contracts for these services during the incident response period. In October 2015, OMB published a Cyber Security Strategy and Implementation Plan (CSIP) for the federal civilian government agencies.[71] The CSIP included a number of deliverables, including one related to establishing contracting vehicles providing incident response services. A government-wide contracting vehicle for incident response services should be established as soon as possible and *before* another agency faces the same situation as OPM. This will ensure such contracting vehicles have the benefit of competition and provide a robust suite of services to assist agencies in an incident response scenario.

Recommendation 10 – Improve and Update Cybersecurity Requirements for Federal Acquisition

OMB should refocus efforts on improving and updating the current patchwork and outdated cybersecurity requirements in existing federal security and acquisition rules. There have been a number of initiatives launched over the last few years to update and improve cybersecurity requirements in federal acquisition. To date, few of these efforts have been finalized. Thus, the Committee recommends that the Administration prioritize and complete efforts to develop and implement clear cybersecurity requirements for federal acquisition as soon as possible. The importance of the partnership between agencies and federal contractors in securing sensitive data held by agencies and contractor-operated systems cannot be overstated. Existing cybersecurity rules and requirements in federal acquisition are ad hoc, overlapping, potentially conflict and are in need of updating.

In February 2013, the President issued Executive Order 13636, *Improving Critical Infrastructure Cybersecurity* and Presidential Policy Directive (PPD) 21, *Critical Infrastructure Security and Reliance*, that directed agencies to complete a broad range of tasks to enhance national

---

[70] *What is an Employee Assistance Program*, U.S. OFFICE OF PERS. MGMT, available at: https://www.opm.gov/faqs/QA.aspx?fid=4313c618-a96e-4c8e-b078-1f76912a10d9&pid=2c2b1e5b-6ff1-4940-b478-34039a1e1174.

[71] Memorandum from Shaun Donovan, Dir., and Tony Scott, Fed. Chief Info. Officer, Office of Mgmt. & Budget, Exec. Office of the President, to Agency Heads, M-16-04, *Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government* (Oct. 30, 2015) available at: https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf.

cybersecurity and resilience.[72] One group of deliverables included a mandate to incorporate cybersecurity requirements into the federal acquisition process. In January 2014, GSA and DOD delivered a report, *Improving Cybersecurity and Reliance through Acquisition* that made recommendations to achieve this objective.[73] These report recommendations have not been implemented to date. The existing framework for cybersecurity requirements in federal acquisition should be reviewed and updated immediately. The January 2014 report recommendations provide useful guidance to inform such an update.

Recommendation 11 – Modernize Existing Legacy Federal Information Technology Assets

Federal agencies should utilize existing tools and Congress should consider new tools to incentivize the transition from legacy to modernized IT solutions. Federal agencies spend over $89 billion annually on IT, with the majority of this spending focused on maintaining and operating legacy IT systems.[74] Over 75 percent of this spending is focused on legacy IT costs.[75]

GAO reported legacy IT investments are becoming increasingly obsolete with outdated software languages and hardware parts that are not supported.[76] Such reliance on legacy IT can result in security vulnerabilities where old software or operating systems are no longer supported by vendors and aging IT infrastructure becomes difficult and expensive to secure. OPM testified before the Committee there "are some of our legacy systems that may not be capable of accepting those types of encryption…"[77]

The solution to this legacy IT challenge must be multifaceted and should include the use of existing and new tools to incentivize modernization. FITARA provides important tools for IT management and acquisition, including facilitating the transition from legacy IT to modernized solutions.[78] In terms of new tools, incentives for agencies to achieve savings through modernization and innovative financing options to promote modernization should be considered.

Recommendation 12 – Agencies Should Consider Using Critical Pay for IT Security Specialists:

Agencies may request and be granted "critical position pay" authority. Agencies may request critical position pay authority only after determining the position in question cannot be filled

---

[72] Exec. Order No. 13636, 78 Fed. Reg. 11739 (Feb. 19, 2013); White House, Press Release, Presidential Policy Directive 21, *Critical Infrastructure Security and Reliance* (Feb. 12, 2013).

[73] Gen. Serv's Admin. & Dep't of Defense, *Improving Cybersecurity and Resilience Through Acquisition* (Nov. 2013), available at: http://www.gsa.gov/portal/mediaId/185367/fileName/improving_cybersecurity_and_resilience_through_acquisition.action.

[74] The annual total of $89 billion for IT understates the federal government's total IT investment because it does not include: (1) DOD classified IT systems; (2) IT investments by 58 independent executive branch agencies (including the CIA); and (3) IT investments by the legislative or judicial branches. Data available through the IT Dashboard, https://itdashboard.gov/ and OMB Office of E-Gov and Information Technology, https://www.whitehouse.gov/omb/e-gov/docs.

[75] Gov't Accountability Office, GAO-16-468, *Information Technology Federal Agencies Need to Address Aging Legacy Systems*, (May 2016).

[76] Id.

[77] *OPM Data Breach: Hearing Before the H. Comm. on Oversight & Gov't Reform* (June 16, 2015) (testimony of Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt.).

[78] National Defense Authorization Act FY 2015, Pub. L. No. 113-291, Title VIII, Subtitle D, 128 Stat. 3292, 3438-50 (Dec. 19, 2014).

with an "exceptionally well-qualified individual" through the use of other available human resource flexibilities and pay authorities. OPM, in consultation with OMB, reviews agency requests. When approving a request, OPM must determine whether the position requires an "extremely high level of expertise" in a "scientific, technical, professional, or administrative field" and is mission critical. Authority is used to *recruit* and/or *retain* exceptional talent, and is capped at 800 positions at any one time. Generally, critical pay may be established up to Cabinet Secretary pay levels ($205,700) and can be increased with approval by the President (but pay and bonus generally cannot exceed the vice president's salary).

The Committee intends to collect more information on the use of critical pay authority in order to conduct appropriate oversight and make adjustments to the authority, and to ensure it provides agencies the necessary flexibility for recruitment and retention of IT security talent. OPM should also consider establishing a pay band for Information Technology Security Specialists.

Recommendation 13 – Improve Federal Recruitment, Training and Retention of Cyber Security Specialists

Recruiting, training, and retaining cyber security specialists should be a critical national security priority. Following the cyberattacks at OPM, the federal CIO and the OMB Director issued a Memorandum concerning a cybersecurity strategy and implementation plan (CSIP) for the federal civilian government.[79] The CSIP included several federal cyber workforce related taskings, including directing:

1. OPM and OMB to compile special hiring authorities by agency that can be used to hire cyber and IT professionals across government.

2. Agencies to participate in OPM's *Cyber Workforce Project* – an effort to code cybersecurity jobs by specialty for the purpose of gaining knowledge about the gaps and challenges in cyber recruitment and retention.

3. DHS to pilot an Automated Cybersecurity Position Description Hiring Tool to assist in implementation of the National Initiative for Cybersecurity Education (NICE) framework, and posting analysis of the cyber workforce on the CIO Council's knowledge portal as a best practice for other agencies to follow.

4. OPM, DHS, and OMB to map the entire cyber workforce across all agencies using the NICE National Cybersecurity Workforce Framework.

5. OPM, DHS, and OMB to develop recommendations for federal workforce training and professional development.

The Administration and Congress must work together to complete these tasks and swiftly take the steps needed to recruit, train, and retain a world class cyber workforce. The Committee notes

[79] Memorandum from Shaun Donovan, Dir., and Tony Scott, Fed. Chief Info. Officer, Office of Mgmt. & Budget, Exec. Office of the President, to Agency Heads, M-16-04, *Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government* (Oct. 30, 2015) available at: https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf.

OMB and OPM jointly transmitted a memorandum to agency heads on a Federal Cybersecurity Workforce Strategy on July 12, 2016 and appreciates this opportunity to continue the dialogue in this area. Finally, Congress and the Administration should consider non-traditional mechanisms to recruit and retain cyber talent. Such mechanisms should complement private sector experience rather than compete with the private sector, recognize the need to quickly hire top talent, and provide an opportunity for public service to those in the private sector.

Table of Names

Office of Personnel Management

Name	Title
Katherine L. Archuleta	Director (May 2013 - July 2015)
Morrell John Berry	Director (April 2009 - April 2013)
Beth F. Cobert	Acting Director (July 2015 - present)
Jason K. Levine	Director of Office of Congressional, Legislative, and Intergovernmental Affairs (August 2015 - present)
Patrick E. McFarland	Inspector General (August 1990-February 2016)
Lisa Schlosser	Acting Chief Information Officer (March - August 2016)
Donna K. Seymour	Chief Information Officer (December 2013-February 2016)
Special Agent in Charge	Office of Inspector General
Linda M. Springer	Director (June 2005-2008)
Clifton ("Clif") N. Triplett	Senior Cyber and Information Technology Advisor
Norbert ("Bert") E. Vint	Acting Inspector General (February 2016 - present) Deputy Inspector General (2006-February 2016)
Jeff P. Wagner	Director of Information Technology Security Operations

Assurance Data, Inc.

Name	Title
Matthew Morrison	President and Chief Executive Officer

Cylance Inc.

Name	Title
Chris Coulter	Managing Director of Incident Response and Forensics
Stuart McClure	Chief Executive Officer, President and Founder
Grant Moerschel	Director of Sales Engineering
Nicholas Warner	Vice President of Worldwide Sales

CyTech Services

Name	Title
Juan Bonilla	Sr. Security Consultant Solutions Engineering (with OPM April 23-May 1, 2015)
Ben Cotton	Chief Executive Officer

SRA

Name	Title
Brendan Saulsbury	Senior Cyber Security Engineer (March 2012 - May 2016)
Jonathan Tonda	OPM Branch Chief, Security Engineering (September 2015-present); Network Security Team Lead, SRA (May 2012-September. 2015)

Imperatis

Name	Title
Patrick Mulvaney	Technical Lead for OPM contract

Misc.

Name	Title
Joel Brenner	Former National Security Agency Senior Counsel
James B. Comey, Jr.	Director of the Federal Bureau of Investigations
Michael V. Hayden	Former Director of the Central Intelligence Agency
James Andrew Lewis	Senior Vice President and Director, Strategic Technologies Program, Center for Strategic and International Studies
Jeff Neal	Former Chief Human Capital Officer at the U.S. Department of Homeland Security
John Schindler	Former National Security Agency officer
Richard A. Spires	Former Chief Information Officer at the U.S. Department of Homeland Security and the Internal Revenue Service

Chapter 1: OPM's IT Security Record Preceding Breaches

The attackers who successfully penetrated the U.S. Office of Personnel Management (OPM) network were sophisticated, but neither their methods nor their ambition was unprecedented. The federal government had been subject to attacks for years by the same or similar groups using similar variants of malware. In fact, OPM had reportedly been hacked in 2012. A vast amount of publicly available information on similar hacks within the past decade was available that should have put OPM on notice. Furthermore, OPM had every incentive to prioritize information security given the volume of sensitive information and PII it holds.

Despite red flags that began as early as 2005, OPM's appropriated IT security funding consistently lagged behind other agencies, its most sensitive data was inadequately protected, and OPM leadership failed to heed recommendations from OPM's IG.

The Rise of Advanced Persistent Threat Hacking

The longstanding OPM cyber security failures that culminated in the theft of personnel records, background investigation data, and fingerprint data began a decade earlier when the federal government was put on notice regarding the nature of the threat. In July 2005, the U.S. Computer Emergency Response Team (US-CERT) issued an alert regarding sophisticated, multi-year efforts in which hackers send targeted, socially-engineered emails (commonly called "spear phishing" emails) for the purpose of having a user download a file that would eventually lead to the exfiltration of sensitive information.[80]

Though the term would not emerge for several years, the alert described what would come to be known as an "advanced persistent threat" (APT) attack. Such attacks are focused on a particular set of high-value assets or physical systems with the explicit purpose of maintaining access and of stealing data over time. Because the attackers are sophisticated, they can learn how to jump from system to system within a given network, often attempting to compromise administrator accounts in order to gain wider and higher levels of access and creating new footholds to maintain their access. When a particular security precaution or obstacle prevents further compromise, the attackers change tactics and maintain a presence on the network until they reach their ultimate objective.

The 2005 US-CERT alert noted that APT attacks had already taken place, and that they often used malware specifically designed to elude anti-virus software and firewalls.[81] The alert specifically noted the use of "McAfee" and "Symantec" names in connection with APT hacks, foreshadowing the "McAfee" name that would later be relevant in the OPM breach.[82]

Since 2005, the federal government has been repeatedly victimized by sophisticated, sustained APT attackers. In 2005, an APT intrusion gathered data from NASA's Vehicle

[80] US-CERT, *Technical Cyber Security Alert TA05-189A: Targeted Trojan Email Attacks* (July 2005).
[81] *Id.*
[82] *Id.*; *see also* Saulsbury Tr. at 60.

Assembly Building.[83] Media outlets reported that Chinese involvement in the hack was likely.[84] In 2007, James A. Lewis of the Center for Strategic and International Studies testified before Congress that intrusions occurred at the Defense Department, State Department and the Commerce Department.[85] In late 2014, a media report catalogued a number of recent attacks against federal entities, including the White House, the State Department, the United States Postal Service, OPM, and the Nuclear Regulatory Commission.[86]

Federal Contractors Holding Sensitive Federal Employee Information Targeted and Attacked

In addition to the targeting of federal agencies, the government contractors that provide services to these agencies and hold sensitive federal employee information increasingly have been targeted by APTs, including several OPM contractors that provide background investigation and healthcare services. The first public reports of data breaches involving OPM contractors surfaced in the summer of 2014.

In August 2014, the largest background investigation contractor, U.S. Investigations Services, LLC (USIS),[87] publicly acknowledged a data breach impacting employees of the Department of Homeland Security.[88] Documents and testimony provided to the Committee indicate that USIS "self-detected" this cyber-attack in June 2014, immediately notified OPM, and by early July 2014 had mitigated the attackers' activity on their systems.[89]

In a June 22, 2015 document provided to the Committee, USIS said based on the results of an investigation, conducted by a company called Stroz Friedberg, it was determined that USIS had been the target of an attack "carried out by a state sponsored actor," commonly referred to as an APT attack.[90] USIS told the Committee that PII for over 31,000 individuals associated with

---

[83] Keith Epstein & Ben Elgin, *Network Security Breaches Plague NASA*, BUS. WEEK, Nov. 20, 2008.
[84] *Id.*
[85] *Holistic Approaches to Cybersecurity to Enable Network Centric Operations: Hearing before the Subcomm. On Terrorism, Unconventional Threats and Capabilities of the H. Comm. On Armed Serv.'s.*, 111th Cong. (Apr. 1, 2008) (statement of James Andrew Lewis).
[86] Jack Moore, *The Year of the Breach: 10 Federal Agency Data Breaches in 2014*, NEXTGOV (Dec. 30, 2014), http://www.nextgov.com/cybersecurity/2014/12/year-breach-10-federal-agency-data-breaches-2014/102066/.
[87] In 1996, USIS was established as a result of the privatization of OPM's Investigations Services and over the years was awarded a series of contracts to perform security clearance background investigations for more than 95 federal agencies. There were a variety of transition issues when the privatization first occurred, including questions about USIS employees' access to government databases. *See* General Accounting Office, GAO/GGD-96-97R, *Privatization of OPM's Investigations Service* (Aug. 22, 1996). In September 2014, OPM decided to end these contracts with USIS. In early 2015, USIS' parent company filed for bankruptcy. *See* Jill Aitoro, *It is Official: USIS is No More with Planned Altegrity Bankruptcy*, WASH. BUS. J., Feb. 4, 2015, http://www.bizjournals.com/washington/blog/fedbiz_daily/2015/02/it-s-official-usis-isno-more-with-planned.html.
[88] Ellen Nakashima, *DHS Contractor Suffers Major Computer Breach, Officials Say*, WASH. POST, Aug. 6, 2014, available at: https://www.washingtonpost.com/world/national-security/dhs-contractor-suffers-major-computer-breach-officials-say/2014/08/06/8ed131b4-1d89-11e4-ae54-0cfe1f974f8a_story.html.
[89] *Hearing on OPM Data Breach: Part II* (statement of Robert Giannetta, Chief Info. Officer, U.S. Investigations Services. LLC).
[90] Letter from Counsel for U.S. Investigations Serv's, LLC (USIS) to the Hon. Elijah E. Cummings, Ranking Member, H. Comm. on Oversight & Gov't Reform (June 22, 2015); *Id*, Ex. 12, (Stroz Friedberg Summary of Investigation (Dec. 2014).

USIS background investigation work for Customs and Border Protection, the National Geospatial-Intelligence Agency, Immigration and Customs Enforcement, and the U.S. Capitol Police "may have suffered compromise in the cyber-attack."[91] USIS indicated this APT began in in late December 2013 and the last attacker activity was observed on July 4, 2014.[92] The USIS investigation also determined that this APT was focused on access to computer systems related to the background investigations business of USIS, which should have made it very clear to all stakeholders that the target was background investigation data.[93]

As a consequence of the USIS activity in the summer of 2014, US-CERT visited the facilities of KeyPoint Government Solutions (KeyPoint) to do a network assessment, which found items of concern that prompted additional review.[94] In December 2014, press reports indicated that KeyPoint had been breached resulting in the possible PII exposure of over 48,000 federal employees.[95] In June 2015, KeyPoint CEO Eric Hess testified before the Committee saying, "there was an individual who had an OPM account that happened to be a KeyPoint employee and that the credentials of that individual were compromised to gain access to OPM."[96] At the time of the 2015 data breach, OPM gave contractors a username and password and investigators would log-in with this OPM credential.[97]

In addition, OPM contractors holding sensitive healthcare information of federal employees have been the targets of APTs. In February 2015, Anthem, one of the largest health insurers in the country and provides coverage for 1.3 million federal employees, announced a data breach involving 80 million records of current and former customers and employees.[98] Then in March 2015, Premera, another health insurance company that has an OPM contract (covering about 130,000 federal workers in Washington state and Alaska), announced a data

---

[91] Letter from Counsel for U.S. Investigations Serv's, LLC (USIS) to the Hon. Elijah E. Cummings, Ranking Member, H. Comm. on Oversight & Gov't Reform at 5 (June 22, 2015).

[92] *Id.* at 5-6. In describing USIS activities related to the June 2014 discovery, USIS noted that an employee of the forensic investigation firm (Stroz Friedberg) they hired attempted to provide US-CERT additional forensic copies of hard drives with evidence of the attack on September 9, 2014, but the US-CERT employee declined saying "US-CERT [was] on a stand down." *Id.* Ex. 6.

[93] *Id.* at 6; *Id.* Ex. 12 Stroz Friedberg Summary of Investigation (Dec. 2014).

[94] *Hearing on OPM Data Breach: Part II* (statement of Ann Barron-DiCamillo, US-CERT Director).

[95] *See e.g.*, Christian Davenport, *KeyPoint Network Breach Could Affect Thousands of Federal Workers*, WASH. POST, Dec. 18, 2014, https://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.

[96] *Hearing on OPM Data Breach: Part II* (statement of Eric Hess, CEO KeyPoint Government Solutions); On June 29, 2015, the American Federation of Government Employees (AFGE) sued OPM over the data breach and also named KeyPoint as a defendant in the lawsuit.

[97] Saulsbury Tr. at 70-71. Wagner, the OPM Director of IT Security Operations said multiple credentials were compromised during the 2015 incident, but a KeyPoint credential was likely used for the initial attack vector. Wagner added "the adversary, utilizing a hosting server in California, created their own FIS [Federal Investigator Service, background] investigator laptop virtually. They built a virtual machine on the hosting server that mimicked and looked like a FIS investigator's laptop…and they utilized a compromise key point user credential to enter the network through the FIS contractor VPN portal." Wagner Tr. at 86, 128.

[98] Reed Abelson & Matthew Goldstein, *Millions of Anthem Customers Targeted in Cyberattack*, N.Y. TIMES, Feb. 5, 2015, available at: http://www.nytimes.com/2015/02/05/business/hackers-breached-data-of-millions-insurer-says.html?_r=0; Aliya Sternstein, *OPM Monitoring Anthem Hack; Feds Might be Affected* (Feb. 5, 2015) available at: http://www.nextgov.com/cybersecurity/2015/02/exclusive-opm-monitoring-anthem-hack-breach-could-impact-13m-feds/104700/.

breach that exposed medical data and financial information for 11 million customers.[99] These attacks highlight the persistent target that federal employee data presents and the need to secure such data – whether it is maintained in a federal or a contractor-operating IT system.

OPM, as well as other agencies, faces the challenge of securing their systems as well as overseeing the systems that government contractors operate on behalf of the government. In a 2014 report, GAO found that while agencies established security requirements and planned for assessments, the agencies reviewed (including OPM) failed to consistently oversee the execution and review of these assessments.[100] In response to GAO's recommendation to OPM "to develop, document and implement oversight procedures for ensuring that a system test is fully executed for each contractor-operator system," OPM promised to review "existing security policies and procedures" to enhance their oversight.[101] According to GAO's website, this recommendation remains open.[102]

In the case of the OPM background investigation contractors who experienced data breaches in 2014 and 2015, OPM had approved IT security plans for both USIS and KeyPoint.[103] In April 2015, GAO repeated the message about the need to address the cybersecurity challenge of ensuring effective oversight of contractors' implementation of security controls for systems contractors operate on behalf of agencies.[104] Based on testimony and documents submitted to the Committee, the record indicates that OPM had not informed USIS or KeyPoint about the March 2014 data breach before it became public.[105] It is unclear whether the attack could have been mitigated if OPM had informed their background investigation contractors, but given the threat environment and the background investigation systems targeted, it would have been prudent to alert the contractors – immediately.[106]

---

[99] *Premera Blue Cross Says Data Breach Exposed Medical Data* , N.Y. TIMES, Mar. 17, 2015, http://www.nytimes.com/2015/03/18/business/premera-blue-cross-says-data-breach-exposed-medical-data.html; Elise Viebeck, *Federal Workers Might be Victims of Premera Data Breach*, THE HILL, Mar. 19, 2015, http://thehill.com/policy/cybersecurity/236266-federal-workers-might-be-victims-of-premera-breach.

[100] Gov't Accountability Office, GAO-14-612, *Agencies Need to Improve Oversight of Contractor Controls* (Aug. 2014), http://www.gao.gov/assets/670/665246.pdf.

[101] Gov't Accountability Office, GAO-14-612, *Agencies Need to Improve Oversight of Contractor Controls* 36 (Aug. 2014), http://www.gao.gov/assets/670/665246.pdf.

[102] *Open Recommendations for GAO-14-612, Agencies Need to Improve Oversight of Contractor Controls* GOV'T ACCOUNTABILITY OFFICE (last visited July 2, 2016), (http://www.gao.gov/recommendations/search?searched=1&hide_order_by_block=1&expand=&openrecs=&rows=10&now_sort=score+desc&page_name=main&q=GAO-14-612&field=rptno_ts

[103] *Hearing on OPM Data Breach: Part II* (testimony by Robert Giannetta, Chief Info. Officer, U.S. Investigations Services, LLC); Letter to the Hon. Elijah E. Cummings, Ranking Member, H. Comm. on Oversight and Gov't Reform from Counsel for U.S. Investigations Services, LLC (USIS) (June 22, 2015), Ex. 8, 9, 10 (ATOs signed by OPM and May 2014 OPM Site Survey Assessment Form); *Hearing on OPM Data Breach: Part II* (statement of Eric Hess, CEO KeyPoint Government Solutions); Email from KeyPoint Counsel to Majority Staff, H. Comm. on Oversight & Gov't Reform (Feb. 22, 2016) (on file with the Committee).

[104] *Enhancing Cybersecurity of Third Party Contractors and Vendors*: *Hearing Before H. Comm. on Oversight & Gov't Reform,* 114th Cong. (Apr. 22, 2015) (testimony of Gregory C. Wilshusen, Dir. Info. Sec. Issues, Gov't Accountability Office).

[105] *Hearing on OPM Data Breach: Part II* (statement of Robert Giannetta, Chief Info. Officer, U.S. Investigations Serv's, LLC). Despite a contractual obligation to notify contractors immediately of a "new or unanticipated threat or hazard," OPM did not notify their contractors (KeyPoint and USIS) of the March 2014 incident. *Id*

[106] *Hearing on OPM Data Breach: Part II* (Rep. Gowdy questioning of OPM contractors and OPM officials on the definition of "immediately.").

Agencies today rely on federal contractors to operate IT systems on behalf of the federal government and must access federal systems in order to perform services for the federal government. The potential risk of unauthorized access to IT systems operated by federal contractors on behalf of the federal government or contractors' IT systems should not have been surprising to OPM in the years leading up to the data breaches.

Federal Initiatives to Increase Information Security in Response to Increasing Attacks

As the first warnings of APT attacks began in 2005, the federal government was beginning to strengthen access controls. On August 5, 2005, OMB issued guidance to implement HSPD-12,[107] a Directive requiring the development and implementation of a mandatory, government-wide standard for secure and reliable forms of identification for federal employees and contractors. The guidance ("Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors") advised the heads of all departments and agencies that "[i]nconsistent agency approaches to facility security and computer security are inefficient and costly, and increase risks to the Federal government."[108] The Administration issued HSPD-12 implementation guidance in the immediate years after the 2005 Directive was issued.[109]

In response to multiple attacks, in 2008, the federal government began a major new initiative to improve the security of its systems.[110] Meanwhile, attacks on federal systems continued and increased in volume and sophistication. Federal agencies only needed to look at attacks on government contractors and other private sector entities for a playbook about what they needed to able to counteract. In 2009, Chinese groups with ties to the People's Liberation Army reportedly carried out dozens of APT attacks against, *inter alia*, Northrop Grumman, Lockheed Martin, and Dow Chemical.[111]

---

[107] Memorandum from Joshua Bolton, Dir. Office of Mgmt. & Budget, Exec. Office of the President, to Dep't and Agency Heads, M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors* (Aug. 5, 2005). On August 27, 2004, the President signed HSPD-12 "Policy for a Common Identification Standard for Federal Employees and Contractors" (the Directive).

[108] Memorandum from Joshua Bolton, Dir. Office of Mgmt. & Budget, Exec. Office of the President, to Dep't and Agency Heads, M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors* (Aug. 5, 2005).

[109] Memorandum from Karen S. Evans, Admin'r, Office of E-Gov't & Info. Tech., Exec. Office of the President, to Chief Info. Officers, and Senior Agency Officials for Privacy, M-06-06, *Sample Privacy Documents for Agency Implementation of Homeland Security Presidential Directive (HSPD) 12* (Feb. 17, 2006), https://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2006/m06-06.pdf. *See also* Exec. Office of the President, Press Release, *HSPD-12 Certified Products and Services Now Available for Agency Acquisition* (July 5, 2006), https://georgewbush-whitehouse.archives.gov/omb/pubpress/2006/2006-28.pdf.

[110] National Security Presidential Directive – 54 Cybersecurity Policy (Jan. 8, 2008) available at: https://fas.org/irp/offdocs/nspd/nspd-54.pdf.

[111] Fayyaz Rajpari, *Finding the Advanced Persistent Adversary*, SANS INST. (Sept. 29, 2014), https://www.sans.org/reading-room/whitepapers/hackers/finding-advanced-persistent-adversary-35512.

Four years later, the situation had not improved and appeared to be getting worse. A 2012 white paper by FireEye stated:

> Federal agencies are increasingly the victims of advanced persistent threats, often comprised of multi-staged, coordinated attacks that feature dynamic malware and targeted spear phishing emails. In fact, in spite of massive investments in IT security infrastructure, on a weekly basis, over 95% of organizations have at least 10 malicious infections bypass existing security mechanisms and enter the network. Further, 80% experience more than 100 new infections each week. Every day, mission-critical systems are compromised, and sensitive and classified data is exfiltrated from federal government and civilian networks.[112]

OPM itself was also targeted in the years leading up to the breaches discovered in 2014 and 2015. In May 2012, a hacker reportedly broke into an OPM database and stole 37 user IDs and passwords.[113] That breach was reportedly carried out by a group called "@k0detec," an activist affiliated with the hacking group Anonymous.[114] In 2011, the Department of Homeland Security issued a cybersecurity bulletin that called Anonymous "script kiddies" using "rudimentary" exploits. If true, Anonymous did not need advanced technical proficiency to gain access to an OPM database.[115]

OPM Failed to Recognize the Threat and Implement Effective IT Security Measures When It Mattered

The threat of APTs was well-known throughout the federal government and OPM was a prime target given the sensitive information it held on current and former federal employees and contractors. Thus, OPM should have made information security a top priority. In the years preceding the breaches at OPM in 2014 and 2015, however, information security was just one of several competing agency priorities, and network vulnerabilities became more acute. In late 2013 and early 2014, under Director Katherine Archuleta and CIO Donna Seymour, OPM attempted to re-focus on improving IT security. It did not work. Ineffective leadership and poor decision-making plagued the agency during a critical period in 2014, leaving the agency in a weak position to prevent the breaches.

---

[112] *Cyber Attacks on Government: How APT Attacks are Compromising Federal Agencies and How to Stop Them* FIREEYE (2012), http://www2.fireeye.com/rs/fireye/images/fireeye-cyber-attacks-government.pdf.

[113] Paul Rosenzweig, *The Alarming Trend of Cybersecurity Breaches and Failures in the U.S. Government Continues*, HERITAGE FOUND. (Nov. 13, 2012), available at: http://www.heritage.org/research/reports/2012/11/cybersecurity-breaches-and-failures-in-the-us-government-continue (citing Privacy Rights Clearinghouse Chronology of Data Breaches available at: http://www.privacyrights.org/data-breach/new) ; *see also* Plaintiff's Class Action Complaint and Demand for Jury Trial, 21 (Aug. 14, 2015), Krippendorf v. U.S. Office of Personnel Mgmt., D.D.C. (No, 1:15 CV 01321) at 21 available at: http://blogs.reuters.com/alison-frankel/files/2015/08/krippendorfvopm-complaint.pdf

[114] Lee Johnstone, *U.S. Office of Personnel Management Hacked & Data Leaked by @k0detec*, CYBER WAR NEWS, May 23, 2012, available at: https://www.cyberwarnews.info/2012/05/23/u-s-office-of-personnel-management-hacked-data-leaked-by-k0detec/. That individual also carried out an attack on the Glade County Florida Sheriff's department

[115] Nat'l Cybersecurity & Comm'n Integration Ctr., Dep't of Homeland Sec., Bulletin A-0010-NCCIC - 160020110719.

OPM's Cybersecurity Spending Consistently Trailed Other Federal Agencies

OPM consistently reported spending less than other federal agencies on *cybersecurity*. In FY 2013, FY 2014 and FY 2015, OPM spent seven million each year on cybersecurity—spending that was consistently at the bottom relative to all other agencies that are required to report such expenditures to the Office of Management and Budget.[116] The previous fiscal year, 2012, OPM also lagged behind other federal agencies.

OPM sought additional funds for cybersecurity, but only after US-CERT notified the agency about the damaging breach in 2014. On March 20, 2014, OPM's Computer Incident Response Team (CIRT) received notification from DHS' US-CERT that data was being exfiltrated from OPM's network.[117] In the weeks that followed, OPM leadership would become aware the intrusion led to the breach of background investigation data in OPM systems holding the "crown jewels" of the American federal workforce and national security personnel.[118]

OPM requested additional cybersecurity funding in its FY 2016 Budget Justification (released February 2015), and only then (ten years after OPM took over the background investigation function) acknowledged it was a target rich environment. In a February 2, 2015 letter to the House Appropriations Subcommittee on Financial Services and General Government concerning its budget request, then-Director Katherine Archuleta noted: "OPM's FY2016 request is $32 million above our FY 2015 appropriation. Most of these funds will be directed towards investments in IT network infrastructure and security. As a proprietor of sensitive data—including personally identifiable information for 32 million federal employees and retirees—OPM has an obligation to maintain contemporary and robust cybersecurity controls."[119]

After years of neglect, the request for increased funding in February 2015 was too little too late. It came more than one year after attackers stole security documents that provided a roadmap to OPM's systems.[120] And the request came after hackers had already successfully exfiltrated sensitive data, including background investigations data in July and August of 2014 and federal employee personnel records in December 2014.[121]

---

[116] *See Infra*, Report Appendix: Cyber security Spending at OPM (Fiscal Years 2012-2015); *see also* Office of Mgmt. & Budget, Exec. Office of the President, *Annual Report to Congress: Federal Information Security Management Act* 82 (Mar. 18, 2016) available at: https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy_2015_fisma_report_to_congress_03_18_2016.pdf. *See also* Office of Mgmt. & Budget, Exec. Office of the President, *Annual Report to Congress: Federal Information Security Management Act* 83 (Feb. 27, 2015) available at: https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy14_fisma_report_02_27_2015.pdf.

[117] June 2014 OPM Incident Report at HOGR0818-001233.

[118] June 2014 OPM Incident Report at HOGR0818 -001245.

[119] U.S. Office of Pers. Mgmt., *OPM Congressional Budget Justification Performance Budget FY2016*, at 2 (Feb. 2015), https://www.opm.gov/about-us/budget-performance/budgets/congressional-budget-justification-fy2016.pdf.

[120] June 2014 OPM Incident Report, *at* HOGR0818 -001242.

[121] OPM Cybersecurity Events Timeline.

OPM Attempts to Balance IT Security with Competing Priorities

The year 2005 was a key year for both OPM and federal cybersecurity. The IG and US-CERT issued a general technical alert, which should have made OPM aware of the need to increase IT security in the face of increasing APT threats,[122] and OMB was gearing up to announce and begin implementation of HSPD-12.[123] The OPM IG also issued a warning in a semiannual report that would be repeated in subsequent reports. It warned:

> OPM relies on computer technologies and information systems to administer programs that distribute health and retirement benefits to millions of current and former federal employees and eligible family members. Any breakdowns or malicious attacks (e.g., hacking, worms or viruses) affecting these federal computer based programs could compromise efficiency and effectiveness and ultimately increase the cost to the American taxpayer.[124]

Amidst efforts to fortify federal cybersecurity, OPM was also working in 2005 to assume responsibility for the processing and storage of federal background investigations. OPM accepted the transfer of the Personnel Security Investigations function and personnel from the Department of Defense's Defense Security Service (DSS)—as authorized by the National Defense Authorization Act of 2004 (P.L. 108-136).[125] The transfer from DSS to OPM's Federal Investigative Services (FIS) division "brought under one roof a unit that is conducting 90 percent of background investigations for the entire Federal Government."[126]

Congress applied pressure on OPM to process the background investigation caseload more efficiently by tasking FIS with meeting timeframes imposed under The Intelligence Reform and Terrorism Prevention Act (P.L. 108-458).[127] This was an important function in the wake of

---

[122] US-CERT, *Technical Cyber Security Alert TA05-189A: Targeted Trojan Email Attacks* (July 2005).

[123] Memorandum from Joshua Bolton, Dir. Office of Mgmt. & Budget, Exec. Office of the President, to Dep't and Agency Heads, M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors* (Aug. 5, 2005). On August 27, 2004, the President signed HSPD-12 "Policy for a Common Identification Standard for Federal Employees and Contractors" (the Directive).

[124] Office of the Inspector Gen., U.S. Office of Pers. Mgmt., *Semiannual Report to Congress October 1, 2004 – March 31, 2005* 11 (May 1, 2005) available at: https://www.opm.gov/news/reports-publications/semi-annual-reports/sar32.pdf.

[125] U.S. Office of Pers. Mgmt., *FY2008 Congressional Budget Justification Performance Budget* 9 (Feb. 5, 2007) available at: https://www.opm.gov/about-us/budget-performance/budgets/2008-budget.pdf. U.S. Office of Pers. Mgmt., Press Release, *OPM Consolidates Bulk of Federal Security Clearance Process with Transfer of Over 1,800 Employees from Defense Department: Vast Majority of Federal Background Investigations to be Centered at OPM* (Nov. 22, 2004) ("The U.S. Office of Personnel Management and Department of Defense announced today the transfer of over 1,800 personnel security investigation staff from DoD to OPM. This move will consolidate the vast majority of background investigations for the Federal government with OPM.").

[126] U.S. Office of Pers. Mgmt., *FY2008 Congressional Budget Justification Performance Budget* 9 (Feb. 5, 2007) available at: https://www.opm.gov/about-us/budget-performance/budgets/2008-budget.pdf.

[127] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 50 U.S.C. § 3341(g) (2012); *see also* Rebeca Laflure, *How Congress Screwed Up America's Security Clearance System*, FOREIGN POLICY, Oct. 1, 2013 available at: http://foreignpolicy.com/2013/10/01/how-congress-screwed-up-americas-security-clearance-

the terrorist attacks in September 11, 2001. Various federal agencies and defense contractors increased their counter-terrorism staff.[128] That staffing surge caused a backlog in processing background investigations. The backlog was at least 188,000 by 2004.[129] The Intelligence Reform and Terrorism Prevention Act (P.L. 108-458) required that 90 percent of clearance applications had to be resolved within 60 days by 2009, a reduction of 84 percent from the then-375 day average wait time.[130]

Clearing the background investigation backlog was a priority, but there was also a clear need for OPM to prioritize the information security of its data. Over the 2005-2007 timeframe, the IG's annual auditing identified weaknesses in the security of the agency's information systems which would deteriorate to "material weakness" status in 2007.[131]

In March 2008, the IG's *Semiannual Report to Congress* recognized a need for the agency to focus on protecting sensitive information and PII over the long-term:[132]

> Unfortunately, in today's high tech world, inappropriate access to this sensitive information can lead to adverse consequences for the American public we are sworn to protect and serve. Consequently, the Office of the Inspector General (OIG) has identified and reported the protection of personally identifiable information as a top management challenge for the U.S. Office of Personnel Management (OPM), and we believe it is a challenge that will be ongoing because of the dynamic and ever-evolving nature of information security.
>
> Recognizing the adverse consequences of lost or stolen PII, including substantial harm, embarrassment and inconvenience to individuals, as well as potential identity theft, OPM's Director, the Honorable Linda M. Springer, initiated a series of actions beginning last fall. She wanted to make sure that all OPM employees clearly understood what PII meant, the importance of protecting PII, and their responsibilities in protecting it.[133]

---

system/; U.S. Office of Pers. Mgmt., *FY2008 Congressional Budget Justification Performance Budget* 9 (Feb. 5, 2007), https://www.opm.gov/about-us/budget-performance/budgets/2008-budget.pdf.

[128] *See, e.g.*, Rebeca Laflure, *How Congress Screwed Up America's Security Clearance System*, FOREIGN POLICY (Oct. 1, 2013) available at: http://foreignpolicy.com/2013/10/01/how-congress-screwed-up-americas-security-clearance-system/.

[129] *Id.*

[130] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 50 U.S.C. § 3341(g) (2012); *see also* Rebeca Laflure, *How Congress Screwed Up America's Security Clearance System*, FOREIGN POLICY, Oct. 1, 2013, http://foreignpolicy.com/2013/10/01/how-congress-screwed-up-americas-security-clearance-system/.

[131] Office of Inspector Gen., U.S. Office of Pers. Mgmt., *Semiannual Report to Congress April 1, 2007 – September 30, 2007*, at 10 (Sept. 2007) available at: https://www.opm.gov/news/reports-publications/semi-annual-reports/sar37.pdf.

[132] Office of Inspector Gen., U.S. Office of Pers. Mgmt., *Semiannual Report to Congress October 1, 2007 to March 31, 2008*, at i (Mar. 2008) available at: https://www.opm.gov/news/reports-publications/semi-annual-reports/sar38.pdf.

[133] Office of Inspector Gen., U.S. Office of Pers. Mgmt., *Semiannual Report to Congress October 1, 2007 to March 31, 2008*, at I (Mar. 2008) available at: https://www.opm.gov/news/reports-publications/semi-annual-reports/sar38.pdf. When the agency made a push in 2008 to ensure "all OPM employees clearly understand what PII meant, the importance of protecting PII, and their responsibilities in protecting it", OPM security staff that were

In the fall of 2008, however, the IG reported that the material weakness from the prior year had not been fully addressed, and that it had "some significant concerns" with aspects of the agency's information security program.[134] The IG warned that major elements of policies had not been updated in five years, found significant deficiencies existing in the control structure of OPM's management of major system certification and accreditation, as well as in the plan of action and milestones process, and that the agency operated without a permanent IT security officer for over six months.[135]

In the spring of 2009, OPM underwent a leadership transition. At John Berry's Senate confirmation hearing in March 2009, Mr. Berry was questioned extensively on the security clearance backlog,[136] however, Congress did not pose any questions to him about information security.[137]

Berry was confirmed in April 2009,[138] and in September 2009 he testified at length on the need to modernize the security clearance system and to eliminate the clearance backlog.[139] His prepared testimony noted that OPM's work to improve background investigation processing would include efforts to strengthen access controls. Berry testified:

> We are working to bring the benefits of access to the verification system to new user types to support agencies in Personal Identity Verification (PIV) credentialing. We are working with the stakeholder community to identify potential enhancement to the verification system to permit greater reciprocity. We are developing a web-based automated tool to assist agencies in identifying the appropriate level of investigation.[140]

Meanwhile in September 2009, the IG reported that the state of information security at OPM was worsening. The IG stated:

> In our FY 2007 and 2008 FISMA audit reports, we reported the lack of policies and procedures as a material weakness. While some progress was made in FY 2009, detailed guidance is still lacking. . . This year, we

---

key to the 2014 and 2015 breach response were already working at OPM. For example, Jeff Wagner, OPM's current Director of IT Security Operations, began working at OPM in June 2006. In transcribed interviews, Mr. Wagner also admitted that he had been on a Performance Improvement Plan (PIP) in 2012 or 2013. He said, "I believe the PIP that I was placed on was because, in my aggressive nature towards IT security, I had offended a few people." *See* Wagner Resume, at 000001 (OPM Production: Aug. 28, 2015); Wagner Tr. at 141-142.

[134] Office of Inspector Gen., U.S. Office of Pers. Mgmt., *Semiannual Report to Congress April 1, 2008 – September 30, 2008*, at 16 (2008) available at: https://www.opm.gov/news/reports-publications/semi-annual-reports/sar39.pdf.

[135] *Id.*

[136] *Nomination of Hon. M. John Berry to be Director, Office of Personnel Management: Hearing Before the S. Comm. on Homeland Sec. & Gov't Affairs,* 111th Cong. (Mar. 26, 2009).

[137] *Id.*

[138] U.S. Office of Pers. Mgmt., Press Release, *John Berry Confirmed as OPM Director* (Apr. 3, 2009) https://www.opm.gov/news/releases/2009/04/john-berry-confirmed-as-opm-director/.

[139] *Security Clearance Reform: Moving Forward on Modernization: Hearing Before the Subcomm. on Oversight of Gov't Mgmt, the Fed. Workforce, & D.C. of the S. Comm. On Homeland Sec. & Gov't Affairs*, 111th Cong. (Sept. 15, 2009) (statement of John Berry, Director, U.S. Office of Pers. Mgmt.).

[140] *Id.*

> expanded the material weakness to include the agency's overall information security governance program and included our concerns about the agency's information security management structure. For example, in the last 18 months, there has not been a permanent Senior Agency Information Security Official (SAISO) or a Privacy Program Manager, resulting in a serious decline in the quality of the agency's information security and privacy programs. With the recent appointment of the new SAISO, and the planned Office of Chief Information Officer reorganization which may involve increased staffing levels, we will reevaluate this issue during the FY 2010 FISMA audit.[141]

In the spring of 2010, the IG continued to report "significant concerns" regarding the overall quality of the information security program at OPM.[142] The IG warned that the agency had not fully documented information security policies and procedures or established appropriate roles and responsibilities, and that while an updated Information Security and Privacy Policy was finalized in August 2009, it did not specifically address OPM's IT environment and lacked detailed procedures and implementing guidance.[143] The IG also questioned in 2010 whether OPM leadership was committed to information security over the long-term. The IG stated:

> This year we expanded the material weakness to include the agency's overall information security governance program and incorporated our concerns about the agency's information security management structure. . . . The agency appointed a new SAISO in September 2009; however, the individual left in January 2010. Another new SAISO was appointed in late April 2010. With a new Chief Information Officer also recently selected, OPM may finally be in a position to make long needed improvements to its IT security program. However, given this turbulent history it remains to be seen whether senior management is fully committed to strong IT security governance for the long term."[144]

In 2012, OPM Director Berry ordered the centralization of IT security duties to a team within OPM's Office of Chief Information Officer (OCIO). In March 2012, the IG reported that "Our audit showed that the agency continues to struggle with improving the quality of its information security program."[145] The IG also found that the agency's OCIO lacked the authority it needed to manage security matters effectively, and that the agency needed to move to a more centralized system "because the fundamental design of the program is flawed."[146] The IG

---

[141] Office of Inspector Gen., U.S. Office of Pers. Mgmt., *Semiannual Report to Congress April 1, 2009 to September 30, 2009*, at 6-7 (Sept. 2009), https://www.opm.gov/news/reports-publications/semi-annual-reports/sar41.pdf.
[142] Office of Inspector Gen., U.S. Office of Pers. Mgmt., *Semiannual Report to Congress October 1, 2009 – March 31*, 2010, at 7-8 (Mar. 2010), https://www.opm.gov/news/reports-publications/semi-annual-reports/sar42.pdf.
[143] *Id.*
[144] *Id.*
[145] Office of Inspector Gen., U.S. Office of Pers. Mgmt., *Semiannual Report to Congress October 1, 2011 to March 31, 2012*, at 7 (Mar. 2012), https://www.opm.gov/news/reports-publications/semi-annual-reports/sar46.pdf.
[146] U.S. Office of Personnel Mgmt. Office of Inspector General *Semiannual Report to Congress October 1, 2012 to March 31, 2013*, at 8-9 (Mar. 2013) available at: https://www.opm.gov/news/reports-publications/semi-annual-reports/sar48.pdf.

pointed out that OPM's "designated security officers" were appointed by, and report to, the program offices that own the systems, but "very few of the DSOs have any background in information security, and most are only managing their security responsibilities as a secondary duty to their primary job function."[147] The IG found that IT security at OPM was limited because "the OCIO has no authority to enforce security requirements" and concluded:

> IT security is a shared responsibility between the OCIO and program offices. The OCIO is responsible for overall information security governance while program offices are responsible for the security of the systems that they own. There is a balance that must be maintained between a consolidated and a distributed approach to managing IT security, but it is our opinion that OPM's approach is too decentralized. OPM program offices should continue to be responsible for maintaining security of the systems that they own, but the DSO responsibility for documenting, testing, and monitoring system security should be centralized within the OCIO.[148]

In other words, there were increasing calls for centralizing and fortifying authority and power under the OCIO by the OIG. By the end of FY2013, the centralized structure for information system security officers remained understaffed and hampered by budget restrictions.[149] And in 2013, as the agency prepared to transition to new leadership, the IG released two key reports. First, its newest FISMA audit found that the security of information systems remained a material weakness.[150]

Second, the IG also issued a warning about the information system where background investigation materials are stored. In June 2013, the IG audited OPM's Federal Investigative Services' Personnel Investigations Processing System (PIPS). The IG made clear the importance of this system:

> Approximately 15 million records of investigations conducted by and for OPM, the Federal Bureau of Investigations (FBI), the U.S. Department of State, the U.S. Secret Service, and other customer agencies are maintained in PIPS. Furthermore, the PIPS system interfaces with several other FIS systems to process applications while its data flow relies on both the OPM Local Area Network/ Wide Area Network (LAN/WAN) and Enterprise Server Infrastructure (ESI) general support systems.[151]

* * *

---

[147] *Id.*

[148] *Id.*

[149] Office of Inspector Gen., U.S. Office of Pers. Mgmt., *Federal Information Security Management Act Audit FY 2013*, at 5 (Nov. 21, 2013), https://www.opm.gov/our-inspector-general/reports/2013/federal-information-security-management-act-audit-fy-2013-4a-ci-00-13-021.pdf.

[150] Office of Inspector Gen., U.S. Office of Pers. Mgmt., *Semiannual Report to Congress October 1, 2013 to March 31, 2014*, at 10 (Mar. 2014), https://www.opm.gov/news/reports-publications/semi-annual-reports/sar50.pdf.

[151] Office of Inspector Gen., U.S. Office of Pers. Mgmt., *Semiannual Report to Congress April 1, 2013 to September 30, 2013*, at 7 (Sept. 2013) available at: https://www.opm.gov/news/reports-publications/semi-annual-reports/sar49.pdf.

> In the case of PIPS, we found that there were a number of controls inappropriately labeled in the system security plan as common or inherited. As a result, these **controls were never tested**, increasing the risk that these controls may not be functioning as intended, and therefore **posing a potential security threat to the system**. This omission is particularly concerning given the purpose of the system and the nature of the data the system contains.[152]

The IG's warning about the weakness in PIPS and the need to protect the background investigations data was prescient. The IG's warnings were in effect when, in 2013, the agency welcomed new senior leadership.

The Katherine Archuleta and Donna Seymour Era

On May 23, 2013, Katherine Archuleta was nominated to serve as Director of OPM.[153] The U.S. Senate confirmed Archuleta on October 30, 2013,[154] and she was sworn into office on November 4, 2013.[155] Archuleta was a former teacher, public administrator, community leader from Colorado and the National Political Director for President Obama's reelection campaign.[156] Shortly thereafter, in December 2013, Donna Seymour began her tenure as OPM's CIO.[157]

During her Senate confirmation hearing on July 16, 2013, Archuleta made a commitment to work with her senior management team to create a plan for modernizing IT within 100 days of assuming office, and to identify new IT leadership using existing agency expertise and with advice from government experts.[158]

As Archuleta and Seymour began their tenure, IT modernization was a key part of the Director's early agenda. Director Archuleta announced a new *Strategic Information Technology*

---

[152] *Id.*

[153] White House, Press Release, *President Obama Announces His Intent to Nominate Katherine Archuleta as Director of the Office of Personnel Management* (May 23, 2013), https://www.whitehouse.gov/the-press-office/2013/05/23/president-obama-announces-his-intent-nominate-katherine-archuleta-direct.

[154] Lisa Rein, "*Senate Confirms Katherine Archuleta as the Next Federal Personnel Chief*," WASH. POST, Oct. 30, 2013 available at: https://www.washingtonpost.com/politics/senate-confirms-katherine-archuleta-as-the-next-federal-personnel-chief/2013/10/30/65959bb0-41a6-11e3-a624-41d661b0bb78_story.html.

[155] U.S. Office of Pers. Mgmt., Press Release, *U.S. Office of Pers. Mgmt., Katherine Archuleta Sworn-In as 10th Director of the Office of Personnel Management: Greets Employees as the New Director and Gets to Work* (Nov. 4, 2013) available at: https://www.opm.gov/news/releases/2013/11/katherine-archuleta-sworn-in-as-10th-director-of-the-office-of-personnel-management/.

[156] Cecilia Muñoz, *Welcoming Katherine Archuleta, the First Latina Director of the Office of Personnel Management*, THE WHITE HOUSE (Nov. 4, 2013, 4:39 p.m.) available at: https://www.whitehouse.gov/blog/2013/11/04/welcoming-katherine-archuleta-first-latina-director-office-personnel-management.

[157] Jason Miller, *CIO Shuffle Continues at SBA, DHS, OPM*, FED. NEWS RADIO (Dec. 20, 2013), http://federalnewsradio.com/technology/2013/12/cio-shuffle-continues-at-sba-dhs-opm/.

[158] U.S. Office of Pers. Mgmt., *Strategic Information Technology Plan* (Feb. 2014) available at: https://www.opm.gov/about-us/budget-performance/strategic-plans/strategic-it-plan.pdf.

Plan in 85 working days (127 calendar days after being sworn in on November 4, 2013).[159] The Plan listed "Information Security" as one of six IT "Enabling Initiatives"—that is, initiatives to "provide the strong foundation necessary for successful operation, development, and management of IT that increases accountability, efficiency, and innovation."[160] The sixty-nine page report includes a brief discussion of the background investigation systems,[161] but the overall discussion related to background investigations focused largely on process reform and automation.[162] The Plan also included two-and-a-half pages on information security, wherein OPM stated it will:

- follow guidance from the *Federal Information Security Management Act*, NIST 800-53 ("Security and Privacy Controls for Federal Information Systems and Organizations");[163]
- follow guidance from OMB to ensure protection of these systems that contain PII and PHI [protected health information];
- work with DHS to implement continuous diagnostic monitoring (CDM) and use information security continuous monitoring (ISCM) tools;
- implement a three-phase plan to carry out its ISCM strategy; and
- attempt to secure additional resources to hire/train IT staff.[164]

Seymour later recounted early efforts to assemble the *Strategic Information Technology Plan* with Archuleta. In June 2014, Seymour testified to the Senate Committee on Homeland Security and Governmental Affairs:

> As Chief Information Officer (CIO) for the Office of Personnel Management (OPM), **I am responsible for the IT and innovative solutions that support OPM's mission** to recruit, retain, and honor a

[159] Joe Davidson, *OPM Unveils IT Plan to Improve Federal Retirement Operations, Recruitment*, WASH. POST, Mar. 10, 2014 available at: https://www.washingtonpost.com/politics/federal_government/opm-unveils-it-plan-to-improve-federal-retirement-operations-recruitment/2014/03/11/aee7db52-a92f-11e3-8599-ce7295b6851c_story.html.

[160] U.S. Office of Pers. Mgmt., *Strategic Information Technology Plan*, at vii (Feb. 2014).

[161] *Id.* at 32.

[162] The Plan's reference to background investigations included one line on security: "The initiative will also support reform in the investigative process and, drawing on the enabling initiative of information security, protect and secure the volume of sensitive information in the EPIC systems [the automated suite of background investigation systems]. U.S. Office of Pers. Mgmt., *Strategic Information Technology Plan* 32 (Feb. 2014).

[163] U.S. Dep't of Commerce, NIST Spec. Publ'n 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (Apr. 2013) available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[164] U.S. Office of Pers. Mgmt., *Strategic Information Technology Plan* at 17-19 (Feb. 2014). Note: While OPM worked to craft the new Plan, key corresponding updates to key internal security guidance and protocols and Authority to Operation (ATOs). For example, OPM's "Incident and Response and Reporting Guide" was not updated—a guide issued in 2009. The Guide contains protocols for responding to breaches, among other things. *See* U.S. Office of Pers. Mgmt., *Incident Response and Reporting Guide* 3 (July 2009). *See also* Special Agent Tr. at 8. The OPM OIG special agent testified on October 6, 2015 that the *Incident Response and Reporting Guide* issued in 2009 was still the guidance in effect at OPM, as of October 2015.

world class workforce. Director Katherine Archuleta tasked me with conducting a thorough assessment of the state of IT at OPM – including how existing systems are managed and how new projects are developed. This process has led us to identify numerous opportunities for improvement in the way we manage IT....

Fulfilling the Director's promise, OPM released a Strategic IT Plan in March 2014. We developed the Strategic IT Plan to ensure our IT supports and aligns to our agency's Strategic Plan and that OPM's mission is fulfilled. It provides a framework for the use of data throughout the human resources lifecycle and establishes enabling successful practices and initiatives that define OPM's IT modernization efforts.

The plan also creates a flexible and sustainable Chief Information Officer (CIO) organization led by a strong senior executive with Federal experience in information technology, program management, and HR policy. OPM also understands that new IT implementation will be done in a way that leverages cybersecurity best practices and protects the personally identifiable information OPM is responsible for.[165]



Donna Seymour testifies to the Committee on Oversight and Government Reform

When Seymour testified before Congress in June 2014, however, **she did not mention that the agency learned in March 2014 of a significant data breach at the agency**; nor did

[165] *A More Efficient and Effective Government: Examining Federal IT Initiatives and the IT Workforce: Hearing Before the Subcomm. on Efficiency & Effectiveness of Fed. Programs & Fed. Workforce of the S. Comm. on Homeland Sec. & Gov't Affairs*, 113th Cong. (June 10, 2014) (statement of Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt.).

she mention that the agency, under her and Archuleta's watch, had spent the previous two months monitoring attackers and remediating a significant incident.[166]

On July 9, 2014, *The New York Times* broke the news, previously unknown to the public, that OPM suffered a breach.[167] *The Times* drew attention to the severe implications of the breach for anyone who had ever applied for a security clearance. The story stated:

> The intrusion at the Office of Personnel Management was particularly disturbing because it oversees a system called e-QIP, in which federal employees applying for security clearances enter their most personal information, including financial data. Federal employees who have had security clearances for some time are often required to update their personal information through the website. The agencies and the contractors use the information from e-QIP to investigate the employees and ultimately determine whether they should be granted security clearances, or have them updated.[168]

While *The Times* immediately grasped the potential implications for the country, OPM's CIO was trumpeting the merits of the agency's IT Modernization plan. In fact, OPM downplayed the damage from the breach to the *The Times*: The story stated:

> But in this case there was no announcement about the attack. 'The administration has never advocated that all intrusions be made public,' said Caitlin Hayden, a spokeswoman for the Obama administration. 'We have advocated that businesses that have suffered an intrusion notify customers if the intruder had access to consumers' personal information. We have also advocated that companies and agencies voluntarily share information about intrusions.'
>
> Ms. Hayden noted that the agency had intrusion-detection systems in place and notified other federal agencies, state and local governments about the attack, then shared relevant threat information with some in the security industry. Four months after the attack, Ms. Hayden said the Obama administration had no reason to believe personally identifiable information for employees was compromised.
>
> 'None of this differs from our normal response to similar threats,' Ms. Hayden said.[169]

---

[166] June 2014 OPM Incident Report; s*ee also, A More Efficient and Effective Government: Examining Federal IT Initiatives and the IT Workforce: Hearing Before the Subcomm. on Efficiency &Effectiveness of Fed. Programs & Fed. Workforce of the S. Comm. on Homeland Sec. & Gov't Affairs*, 113th Cong. (June 10, 2014) (statement of Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt.).

[167] Michael S. Schmidt, David E. Sanger & Nicole Perlroth, *Chinese Hackers Pursue Key Data on U.S. Workers*, N.Y. TIMES, July 9, 2014, available at: http://www.nytimes.com/2014/07/10/world/asia/chinese-hackers-pursue-key-data-on-us-workers.html?_r=0.

[168] *Id.*

[169] *Id.*

Archuleta and Seymour later testified in 2015 that no PII was exfiltrated during the 2014 data breach.[170] Documents and testimony show gaps in OPM's audit logging practices led DHS to conclude the country will never know with complete certainty all of the documents the attackers exfiltrated during the breach discovered in March 2014.[171] It is clear, however, sensitive data was exfiltrated by the hackers.[172] As discussed in the following chapter, OPM watched the attackers steal documents related to OPM IT systems, including PIPs, contractor information, and documents containing names and the last four digits of associated Social Security numbers.[173]

Archuleta and Seymour did make some progress in addressing security governance issues by continuing to centralize IT security responsibility. They committed to make IT a priority with the release of their IT Modernization plan in early 2014, and arguably had more ownership of its IT security at this point than ever before. However, they failed to prioritize data security and implementation of basic cyber hygiene measures at a time when it became critically important to meet the increasing cyber threat.



Katherine Archuleta testifies to the Committee on Oversight and Government Reform

[170] *OPM Data Breach: Part II* (statement of Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt.). During this hearing, then-Director of OPM, Katherine Archuleta, and then-CIO of OPM, Donna Seymour, testified nine times in a single exchange with Chairman Jason Chaffetz that no personally identifiable information was stolen.
[171] June 2014 OPM Incident Report at HOGR0818-001233-1246.
[172] The sensitivity of these documents is evidenced in part by the fact that OPM refused to produce these documents to the Committee in unredacted form until February 16, 2016. The Committee initially requested this information on August 18, 2015.
[173] June 2014 OPM Incident Report at HOGR0818 -001245-1246.

OPM Failed to Prioritize the Security of Key Data and Systems

OPM's failure to prioritize high-value targets like the background investigations data compounded the problems caused by inadequately investing in cybersecurity in the first place. Neither the data held by OPM, nor the access to OPM systems, were adequately protected. Indeed, OPM did not even have a complete IT inventory of servers, databases, and network devices.[174]

Further, on the system level OPM had not implemented multifactor authentication, making weak access controls a vulnerability that attackers were able to exploit.[175] OPM's failure to prioritize multifactor authentication implementation was a key observation that US-CERT made in their analysis of the data breach discovered in 2014.[176]

OPM was pressed about these and other issues during congressional hearings. For example, the background investigations data was not encrypted—encryption is the foundation of data-level security.[177] During a June 16, 2015 hearing before the Committee, Chairman Jason Chaffetz asked Director Archuleta why OPM did not use encryption, an industry best practice, and Director Archuleta said, "It is not feasible to implement on networks that are too old."[178]

Similarly, CIO Seymour told Ranking Member Elijah Cummings that the agency was working to use encryption. She testified:

> OPM has procured the tools, both for encryption of its databases, and we are in the process of applying those tools within our environment. But there are some of our legacy systems that may not be capable of accepting those types of encryption in the environment that they exist in today.[179]

In addition, key systems were also operating in FY 2014 without a valid Security Assessment and Authorization.[180] Also called "ATOs", authorizations to operate/authorities to operate provide a comprehensive assessment of the IT system's security controls. The OPM IG

---

[174] Office of Inspector General, U.S. Office of Pers. Mgmt., Report No. 4A-CI-00-15-011, *Federal Information Security Management Act Audit FY 2014* at i (Nov. 10, 2015) available at: https://www.opm.gov/our-inspector-general/reports/2015/federal-information-security-modernization-act-audit-fy-2015-final-audit-report-4a-ci-00-15-011.pdf

[175] *Information Technology Spending and Data Security at the Office of Personnel Management: Hearing Before the Subcomm. On Financial Serv.'s and Gen. Gov. of the Sen. Comm. on Appropriations,* 114th Cong. (June 23, 2015) (testimony of Richard Spires, former CIO of the Internal Revenue Serv.).

[176] *See Infra* Chapter 2.

[177] *Information Technology Spending and Data Security at the Office of Personnel Management: Hearing Before the Subcomm. On Financial Serv.'s and Gen. Gov. of the Sen. Comm. on Appropriations,* 114th Cong. (June 23, 2015) (testimony of Richard Spires, former CIO of the Internal Revenue Serv.).

[178] *OPM Data Breach, Hearing Before the H. Comm. on Oversight & Gov't Reform*, 114th Cong. (June 16, 2015) (statement of Katherine Archuleta, Dir., U.S. Office of Pers. Mgmt.).

[179] *OPM Data Breach, Hearing Before the H. Comm. on Oversight & Gov't Reform*, 114th Cong. (June 16, 2015) (statement of Katherine Archuleta, Dir., U.S. Office of Pers. Mgmt.).

[180] Office of the Inspector General, U.S. Office of Pers. Mgmt., *Federal Information Security Management Act Audit FY 2014* (Nov. 12, 2014) available at: https://www.opm.gov/our-inspector-general/reports/2014/federal-information-security-management-act-audit-fy-2014-4a-ci-00-14-016.pdf.

considers the authorization process to be a "critical step toward preventing security breaches and data loss."[181]

Of the 21 OPM systems due for reauthorization in FY 2014, 11 were not completed on time and were operating without a valid Authorization,[182] and several were among the most critical, containing the agency's most sensitive information.[183] This led the IG to warn OPM that "The drastic increase in the number of systems operating without a valid Authorization is alarming, and represents a systemic issue of inadequate planning by OPM program offices to authorize the information systems that they own."[184]

FISMA requires agencies to assess the effectiveness of their information security controls, the frequency of which is based on risk but no less than annually.[185] Appendix III of OMB Circular A-130, in place at the time, requires that agencies assess and authorize (formerly referred to as certify and accredit) their systems before placing them into operation and whenever there is a major change to the system, *but no less than every three years thereafter.*[186]

In November 2014, the IG's FISMA audit stated: "We therefore also recommend that OPM consider shutting down systems that do not have a current and valid Authorization."[187] OPM CIO Donna Seymour responded, however, that "The IT Program Managers will work with ISSOs to ensure that OPM systems maintain current ATOs and that there are no interruptions to OPM's mission and operations."[188]

Of the eleven major OPM information systems that were operating without a valid Authorization in FY2014,[189] three of these systems should have been an immediate priority for Director Archuleta and CIO Seymour to ensure were addressed: Personnel Investigations Processing System (PIPS), Enterprise Server Infrastructure (ESI), and the Local Area Network / Wide Area Network (LAN/WAN).

The security of these systems is critical because the flow of background investigation data through PIPs relies on both the OPM LAN/WAN and Enterprise Server Infrastructure (ESI) general support systems. LAN/WAN serves as the hardware and software infrastructure

---

[181] *Id.* at 11.
[182] *Id.* at 9.
[183] E-mail from Office of Pers. Mgmt. Inspector Gen. Staff to House Oversight & Gov't Reform Staff (Dec. 4, 2015) (on file with the Committee).
[184] U.S. Office of Personnel Mgmt. Office of the Inspector General, *Federal Information Security Management Act Audit FY 2014* at 9 (Nov. 12, 2014) available at: https://www.opm.gov/our-inspector-general/reports/2014/federal-information-security-management-act-audit-fy-2014-4a-ci-00-14-016.pdf.
[185] Federal Information Security Management Act of 2002, Pub. L. No. 107-347, 44 U.S.C. § 3541 (2012).
[186] Office of Mgmt. & Budget, Exec. Office of the President, OMB Circular A-130, Management of Federal Information Resources (Nov. 28, 2000) available at: https://www.whitehouse.gov/omb/circulars_a130_a130trans4/; see also U.S. Dep't of Homeland Sec., Security Authorization Process Guide 1 (Mar. 16, 2015) available at: https://www.dhs.gov/sites/default/files/publications/Security%20Authorization%20Process%20Guide_v11_1.pdf.
[187] Office of the Inspector Gen., U.S. Office of Pers. Mgmt., Report No. 4A-CF-00-12-066, *Federal Information Security Management Act Audit FY 2014* at 2, 14 (Nov. 12, 2014) available at: https://www.opm.gov/our-inspector-general/reports/2014/federal-information-security-management-act-audit-fy-2014-4a-ci-00-14-016.pdf.
[188] *Id.*
[189] *Id.* at 9.

environment, supporting systems housed at OPM's Washington, D.C.; Macon, Georgia; and Boyers, PA facilities. LAN/WAN also supports the OPIS (PIPS imaging system)[190] and FTS (Fingerprint Transactional System). ESI is the general mainframe environment that supports PIPS. OPM's mainframe is considered a separate infrastructure or "general support system" from the LAN/WAN. PIPS, LAN/WAN and ESI were all operating on expired Authorities to Operate.[191]

The need to prioritize the security of these systems was well-known after the IG warned in June 2013 that PIPS had vulnerabilities, and that the "PIPS system interfaces with several other FIS systems to process applications while its data flow relies on both the OPM Local Area Network/ Wide Area Network (LAN/WAN) and Enterprise Server Infrastructure (ESI) general support systems."[192] However, the ATO for PIPS was not reauthorized in 2014, and the IG's FY2015 FISMA showed that "OPM's management of system Authorizations has deteriorated even further."[193]

Experts from outside OPM also criticized OPM's choices regarding IT security following the breach. On June 23, 2015, Richard Spires, the former CIO of the Internal Revenue Service and at DHS, testified before a Senate Committee on Appropriations' Subcommittee on Financial Services and General Government that OPM should have set better priorities and focused on securing the data itself rather than the systems as an initial priority. Spires stated:

> [I]f I had walked in there [OPM] as the CIO—and, you know, again, I'm speculating a bit, but—and I saw the kinds of lack of protections on very sensitive data, the first thing we would have been working on is how do we protect that data? OK? Not even talking about necessarily the

---

[190] OPIS was also operating with an invalid authorization to operate. *See* Office of Inspector Gen., U.S. Office of Pers. Mgmt., Report No. 4A-IS-00-06-024, *Information Technology Security Controls of the Office of Personnel Management's Personnel Investigations Processing Imaging System* (July 11, 2006); *see also* E-mail from U.S. Office of Pers. Mgmt. Inspector Gen. Staff to House Oversight & Gov't Reform Staff (Dec. 4, 2015) (on file with the Committee).

[191] Office of Inspector Gen., U.S. Office of Pers. Mgmt., Report No. 4A-IS-00-13-022, *Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Personnel Investigations Processing System FY2013* (June 24, 2013) available at: https://www.opm.gov/our-inspector-general/reports/2013/audit-of-the-information-technology-security-controls-of-the-us-office-of-personnel-managements-personnel-investigations-processing-system-fy-2013-4a-is-00-13-022.pdf; Office of Inspector Gen., U.S. Office of Pers. Mgmt., Report No. 4A-CI-OO-ll-016, *Federal Information Security Management Act Audit FY 2012* (Nov. 5, 2012) available at: https://www.opm.gov/our-inspector-general/reports/2012/federal-information-security-management-act-audit-fy-2012.pdf; Office of Inspector Gen., U.S. Office of Pers. Mgmt., Report No. 4A-CI-OO-12-014, *Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Local Area Network / Wide Area Network General Support System FY 2012* (May 16, 2012) available at: https://www.opm.gov/our-inspector-general/reports/2012/audit-of-the-information-technology-security-controls-of-the-office-of-personnel-managements-local-area-network-wide-area-network-general-support-system-fy-2012.pdf.

[192] Office of the Inspector General, U.S. Office of Pers. Mgmt., *Semiannual Report to Congress April 1, 2013 to September 30, 2013*, at 7 (Sept. 2013) available at: https://www.opm.gov/news/reports-publications/semi-annual-reports/sar49.pdf.

[193] Office of Inspector General, U.S. Office of Pers. Mgmt., Report No. 4A-CI-00-15-011, *Federal Information Security Management Act Audit FY 2014* (Nov. 10, 2015) available at: https://www.opm.gov/our-inspector-general/reports/2015/federal-information-security-modernization-act-audit-fy-2015-final-audit-report-4a-ci-00-15-011.pdf.

> systems. How is it we get better protections and then control access to that data better?[194]

Spires also stated that management issues posed a greater obstacle than resource problems in solving IT security problems. Spires testified:

> A focused effort on protecting the sensitive data with the right encryption and the right access-control capabilities, if you put the focus there, I think most federal agencies would have the funds, have the resources to be able to accomplish that.
>
> * * *
>
> Because of the sparse nature of the way IT has been run in a lot of agencies there are so many, let's say, inefficiencies that have crept into this system that I don't believe we effectively spend the IT dollars that we receive. So I believe that with the proper drive towards management you can actually derive a lot of savings from existing budgets.[195]

OPM has long been plagued by management's failure to prioritize information security in practice, and to retain leaders that are committed to information security over the long haul. Years of neglect, compounded by an abject failure of key leaders to make the right decisions at OPM in 2014, led to the worst data breach the federal government has ever experienced.

---

[194] *Information Technology Spending and Data Security at the Office of Personnel Management: Hearing Before the Subcomm. on Financial Serv.'s and General Gov. of the S. Comm. on Appropriations,* 114th Cong. (June 23, 2015) (testimony of Richard Spires, former Chief Info. Officer, Internal Revenue Serv.).

[195] *Id.*

Chapter 2: The First Alarm Bell – Attackers Discovered in 2014 Target Background Information Data and Exfiltrate System-Related Data

In the March 2014, US-CERT alerted OPM to an intrusion that laid the groundwork for the breach of OPM systems holding background investigation data, the "crown jewels" of current and former federal employees, contractors, and national security personnel.[196] OPM considered their response to the data breach, which they learned about from US-CERT in 2014, a success. CIO Donna Seymour touted the response strategy: "one of the things we were able to do immediately at OPM [in 2014] was recognize the problem. We were able to react to it by partnering with DHS . . . to put mitigations in place to better protect information."[197]

However, the data breach of background investigation data and personnel records first announced in June and July of 2015[198] raises serious questions about OPM's response to the data breach discovered in 2014. Documents and testimony obtained by the Committee show successes and failures, but some of the most important questions were unanswerable.

For example, while OPM testified that no personally identifiable information (PII) was exfiltrated during the 2014 data breach,[199] gaps in OPM's audit logging practices led DHS to conclude that the country will never know with complete certainty the universe of documents the attackers exfiltrated.[200] Documents and testimony show the materials exfiltrated from OPM likely would have given an adversary an advantage in hacking OPM's systems.[201] This evidence calls Donna Seymour's testimony into question. She told the Committee "**the adversaries in today's environment are typically [able] to use more modern technologies, and so in this case, potentially our antiquated technologies may have helped [OPM] a little bit.**"[202] In putting forward a "security through obscurity" defense, the CIO downplayed the reality that OPM was facing a determined and sophisticated actor while only having minimal visibility into their environment.

---

[196] June 2014 OPM Incident Report; *see also* David Perera & Joseph Marks, *Newly Disclosed Hack Got "Crown Jewels,"* POLITICO, June 12, 2015, available at: http://www.politico.com/story/2015/06/hackers-federal-employees-security-background-checks-118954.

[197] *Enhancing Cybersecurity of Third-Party Contractors and Vendors: Hearing Before the H. Comm. on Oversight & Gov't Reform*, 114th Cong. (Apr. 22, 2015) (Question by Mr. Cummings).

[198] U.S. Office of Pers. Mgmt., Press Release, *OPM to Notify Employees of Cybersecurity Incident* (June 4, 2015) available at: https://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident/; U.S. Office of Pers. Mgmt., Press Release, *OPM Announces Steps to Protect Federal Workers and Others From Cyber Threats*, (July 9, 2015) available at: https://www.opm.gov/news/releases/2015/07/opm-announces-steps-to-protect-federal-workers-and-others-from-cyber-threats/.

[199] *Hearing on OPM Data Breach: Part II* (statement of Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt.). During this hearing, then-Director of OPM, Katherine Archuleta, and then-CIO of OPM, Donna Seymour, testified nine times in a single exchange with Chairman Jason Chaffetz that no personally identifiable information was stolen.

[200] June 2014 OPM Incident Report *at* HOGR0818-001233 – 1246.

[201] Saulsbury Tr. at 27-28.

[202] *Enhancing Cybersecurity of Third-Party Contractors and Vendors: Hearing Before the H. Comm. on Oversight & Gov't Reform*, 114th Cong. (2015) (Question by Mr. Cummings).

In the aftermath of their 2014 response, available threat intelligence about the relevant actor groups targeting federal employee information and the types of malware discovered in 2014 also raised the stakes for OPM. In the fall of 2014, Novetta and a number of supporting industry organizations produced a detailed report containing information pertinent to Chinese APT activity with an emphasis on Hikit malware. This malware was found during the 2014 incident response. The Novetta paper specifically looked at the Axiom Threat Actor Group, which according to public reports, was responsible for the OPM data breach discovered in 2014.[203] The analysis warned that among the industries being targeted or infected by Hikit were Western government agencies with responsibility for personnel management. The report also warned that "[w]ithin these targets, Axiom has been observed as going out of its way to ensure continued access regardless of changes to its target's network topology or security controls."[204]

OPM leadership downplayed the significance of the 2014 breach. Instead, OPM should have raised the alarm and recognized this initial attack as a serious and potentially devastating precursor given how close the early attackers got to the background investigation systems and the related data taken during this breach. The following discussion describes OPM's 2014 discovery and incident response efforts, and how Hikit malware was found and sensitive data related to the background investigation function was taken from OPM's systems. Further, this discussion highlights key observations that were made about the weaknesses and vulnerabilities of OPM's IT security during this incident response period.

Discovery & Incident Response for Attackers Discovered in 2014

On March 20, 2014, OPM's Computer Incident Response Team (CIRT) received notification from DHS' US-CERT that data had been exfiltrated from OPM's network.[205] Beginning March 2014 and through May 2014, OPM (in consultation with US-CERT) investigated the incident, monitored the attacker, developed and implemented a mitigation plan, and removed this initial attacker from OPM's system.

US-CERT notified OPM that a third party had reported data being exfiltrated from OPM's system to a known command and control server (C2).[206] Jeffrey Wagner, OPM's Director of IT Security, testified about OPM activities upon notice from US-CERT:

> [T]he initial response [to the 2014 data breach] is a 3/20 call from DHS. All right. So on 3/20 DHS called us and let us know, hey, we think this is bad. We began pulling logs, and records, and things of that nature, and on 3/25 is when we verified that it was a malicious activity.[207]

---

[203] Novetta Operation SMN: Axiom Threat Actor Group Report.
[204] *Id.* 8-9.
[205] June 2014 OPM Incident Report at HOGR0818-001233.
[206] *Id.* OPM contractor Brendan Saulsbury stated that "[the 2014 incident] was first detected by US-CERT via the Einstein appliances that they have on [OPM's] network. And that was communicated to OPM via email." Saulsbury Tr. at 13. The OPM Incident Report states that a "third party" reported the data exfiltration to DHS. June 2014 OPM Incident Report at HOGR0818 -001233. It is possible that both accounts are correct and that the "third party" referenced in the 2014 Incident Report is an Internet Service Provider who reported network activity collected by an Einstein sensor.
[207] Wagner Tr. at 13.

Wagner also described OPM's process for analyzing and elevating information security reporting or alerts to a cybersecurity incident. He stated:

> Once we get forensic evidence that there's actual adversary activity within the environment, it escalates the level of response. So, for instance, on a regular basis we get alerts or reports of an email trying to be sent to us that has a malicious link. It creates an alert. We'll do initial forensics on that alert, and we'll see that our current tools will stop that malicious link from being able to connect or downloading anything. And it de-escalates the situation. So from an incident response perspective, everything rises to a critical level, and then once we have forensics evidence and identify specifically what is going on, and it then escalates into the specific response required.[208]

As OPM's incident response activities began, documents show that as of March 20, 2014, the following facts were among those known to OPM:

- FIS Investigator accounts had been compromised.
- The malicious C2 server was communicating with an OPM server.
- The malicious C2 servers' communications with OPM were encrypted.[209]

During the incident response period, OPM learned the C2 server was connecting with an OPM network monitoring server ([redacted]) between the hours of 10 p.m. and 10 a.m.; then the attackers were using this server and a compromised Windows domain administrator credential to search for PIPs-related files on OPM's network.[210] An initial examination of the network traffic between the [redacted] server and the C2 server found that the communications were encrypted utilizing a four byte XOR key, indicating a specific intent to disguise themselves amongst network traffic.[211]

Brendan Saulsbury, an OPM contractor working in the OPM IT Security Operation group, testified that OPM used the security tool NetWitness to identify what devices on OPM's network were actively communicating, or "beaconing" to the C2 server.[212] Using the network traffic information gathered by NetWitness, Saulsbury was able to design a custom script to "reverse engineer the obfuscation algorithm the attackers were using to mask their traffic so it would not be detected by sensors, like [OPM's] security tools."[213] Saulsbury's team could then

---

[208] *Id.*
[209] June 2014 OPM Incident Report at HOGR0818 -001240.
[210] *Id.* at HOGR0818-001233.
[211] *Id.* An XOR key encryption, or exclusive-or encryption is a form of private key encryption that relies upon a simple binary formula to develop its obfuscation of the underlying data.
[212] Saulsbury Tr. at 39.
[213] Saulsbury Tr. at 40.

observe the infected machines communicating with the C2 server, and also the commands that were being sent down from the "actual attacker sitting at the keyboard."[214]

Thus, OPM and their interagency team were able to identify the adversary's initial foothold in OPM's network—where the attackers had established a persistent presence in the environment. Once it was determined which devices on OPM's network were beaconing to the hackers' C2 server, OPM was in a position to begin a full forensic investigation and look for malware on the compromised machines.[215] On or about March 25, in the words of OPM Director of Security Operations Jeff Wagner, a "critical level"[216] was reached and OPM was able to make a "full determination on the who and what"[217] of the data breach, to know where the hackers are "going, what they are seeing," and most importantly "what [the hackers] are interested in."[218] As a result, OPM determined the incident was malicious on March 25, 2014, moved DHS onsite to assist the response, and began a full monitoring phase to gather information to answer the question of "how."[219]

During the three-month incident response period, OPM undertook a number of other incident response activities. For example, according to US-CERT's 2014 Report timeline, on March 26, 2014 OPM searched for embedded malware on end points at its Washington, D.C. headquarters, at its Boyers, Pennsylvania data center, and at a back-up data center in Macon, Georgia.[220] On March 27, 2014, OPM took steps to remediate the OPM Personnel Investigations Processing System Imaging System (OPIS)—a system that provides an electronic representation of case paper files to expedite the processing of background investigations – and performed this remediation work in late March.[221] On March 28, 2014, in recognition of the fact that OPM did not have the ability to monitor traffic in and out of PIPS – the system that held background investigation data – OPM installed a fiber tap to begin to monitor such traffic. Finally, during this period OPM watched the attackers take sensitive data relating to high-valued targets on OPM's systems, such as the PIPS system.[222] OPM was never able to determine how the adversary initially entered their systems.

Then from late March through April 2014 the incident response team continued to identify additional infected workstations and malware on key systems.[223] Specifically, OPM found Hikit malware on several OPM systems.[224] Hikit is a variant of rootkit malware (which is "an extremely stealthy form of malware designed to hide its malicious processes and programs from the detection of commodity intrusion detection and anti-virus products").[225] As US-CERT

---

[214] Saulsbury Tr. at 40.
[215] Saulsbury Tr. at 39-40.
[216] Wagner Tr. at 13.
[217] June 2014 OPM Incident Report at HOGR0818 -001240.
[218] *Id.*
[219] *Id.*
[220] June 2014 OPM Incident Report at HOGR0818 -001241.
[221] *Id.*; *see also* Office of Pers. Mgmt., *OPM Personnel Investigations Processing System Imaging System (OPIS) Privacy Impact Assessment* available at: https://www.opm.gov/information-management/privacy-policy/privacy-policy/pips-imagingsystem.pdf.
[222] June 2014 OPM Incident Report at HOGR0818-001234.
[223] June 2014 OPM Incident Report at HOGR0818-001241-1242.
[224] June 2014 OPM Incident Report at HOGR0818-001234; *Id.* at Appendix C.
[225] June 2014 OPM Incident Report at HOGR0818-001234.

explained in the June 2014 OPM Incident Report, "HiKit allows the attacker to run commands and perform functions from a remote location as if they had the equivalent of a monitor and keyboard connected to the compromised OPM system."[226]

Time is crucial in an incident response scenario. According to NIST, "organizations should strive to detect and validate malware incidents rapidly because infections can spread through an organization within a matter of minutes."[227] The agency's slow response made matters worse. According to NIST, "minimizing the number of infected systems, which will lessen the magnitude of the recovery effort."[228]

Once the incident was identified and OPM, along with their interagency partners, entered into an advanced monitoring phase necessary intelligence was gathered on the adversaries' tactics, techniques, and procedures, the kind of threat information necessary to harden information security not only at OPM but at other agencies.

Monitoring the Adversary and the May 2014 "Big Bang" to Expel Attackers Discovered in 2014

From March 25, 2014 to May 27, 2014, OPM, upon the advice of US-CERT, engaged in a prolonged intelligence gathering phase. The goal of this advanced monitoring phase was to "carefully observe all of the malicious actors' activities in order to gain an understanding of their tactics, techniques, and procedures (TTPs) as well as to identify all of their other unknown or inactive infected systems within OPM's network."[229] The advanced monitoring of the adversary ended in a "Big Bang" on May 27, 2014—an effort that commenced once the hackers got "too close" to the background investigation material accessible from the PIPS system.[230]

Saulsbury described the comprehensive monitoring strategy during a transcribed interview with Committee investigators. He testified:

> [US-CERT's] advice was to basically do an ongoing investigation and figure out, do our best to find the entire attacker foothold in the network and then remediate them all at once to prevent the attacker from realizing that you are aware of them, and then changing their tactics and techniques to further avoid detection.[231]

Wagner also described the scope of the monitoring phase. He testified that OPM was not just looking for TTPS, but other indicators. Wagner stated:

---

[226] June 2014 OPM Incident Report at HOGR0818-001234.
[227] Peter Mell, Karen Kent & Joseph Nusbaum, Nat'l Inst. of Standards & Tech., Spec. Publication 800-83, *Guide to Malware Incident Prevention and Handling* 3 (Nov. 2005) available at: http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf.
[228] *Id.*
[229] June 2014 OPM Incident Report at HOGR0818 -001233.
[230] Saulsbury Tr. at 26.
[231] Saulsbury Tr. at 25-26.

> You're trying to find specific actions they're doing to give you an indication of what they're doing and what they want. You're also looking for -- as a former pen tester, usually what you try to do to try to prevent people from catching you, is you try to set up other back doors or means in which you can create a persistent attack. It's just making sure you always have a secondary way in.[232]

In US-CERT's June 2014 OPM Incident Report, there is almost a daily catalogue of OPM's monitoring efforts. As part of the monitoring effort, OPM established a series of alerts and system rules to watch the adversary, employing a full packet capture (logging data) tool to gather network traffic between the infected machines and the C2 server.[233] An interagency team, including DHS, FBI, and NSA,[234] was involved in the incident response effort. The team received automatic notifications during the monitoring phase.[235] During this 2014 incident response period, OPM used its existing set of security tools and infrastructure to conduct their monitoring effort.[236]

In addition to monitoring, OPM was prepared to implement preventative measures. For example, Wagner testified that they were instructed to shutoff internet access if any PII was leaving the network.[237] By March 27, 2014, US-CERT reported that OPM had "heightened proactive readiness" and was developing plans for "full shutdown."[238] By April 11, 2014, tactical mitigation strategy and security remediation plans were being developed to eliminate the adversary's foothold on OPM's network.[239] The process of setting up alerts and tipping points, identifying infected workstations, and elevating monitoring technology continued until the "Big Bang" on May 27, 2014.

While the US-CERT timeline is helpful to understand the 2014 incident response activities, some entries illustrate gaps in OPM's visibility into their systems and applications, including the highly sensitive PIPs system – which housed the sensitive background investigation data. For example, the March 28, 2014 timeline entry states OPM "did not have [the] ability to monitor traffic in/out of PIPS – Installed PIPS fiber tap."[240] Wagner responded to this entry by testifying:

> So in that specific instance -- a mainframe functions significantly different

---

[232] Wagner Tr. at 15.
[233] June 2014 OPM Incident Report at HOGR0818 -001240.
[234] Saulsbury Tr. at 43 ("US-CERT brought the NSA Blue Team onsite.").
[235] Wagner Tr. at 59 ("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.").
[236] June 2014 OPM Incident Report at HOGR0818 -001233.
[237] Wagner Tr. at 10 (The question posed to Mr. Wagner was whether or not the security staff at OPM had the authority to make operational decisions; his answer stated that "I guess a good example would be during the 2014 or 2015 breaches, the security operations group was under a standing order from the director that if we indicated that information was leaving, we could shut down the Internet at any time.").
[238] June 2014 OPM Incident Report at HOGR0818 -001241.
[239] *Id.*
[240] *Id.*

> from a standard distributing environment, say Linux, or Windows, or like you have at your home. A mainframe is a giant cloud computer, which runs on a proprietary type operating system, and it communicates in a far different method than a standard distributing environment. So at the time we did not have equipment installed to try to navigate between distributed and mainframe. We had a project to implement these pieces, and what we did is we sped up the project to get the fiber taps installed to be able to set up a communication method to where we could see the traffic as it traversed between the distributing environment and the mainframe environment.[241]

Saulsbury also described OPM's limited ability to monitor Internet traffic during and prior to the 2014 incident. He testified:

> OPM had the ability to monitor traffic going out to the Internet at all times or at least going back prior to the 2014 incident. The reason for putting a network tap on the PIPS segment is to be able to monitor what is called, what we refer to as east-west traffic, so internal-to-internal traffic, from the general network going in and out of PIPS.[242]

It was not until March 31, 2014 that OPM was able to "turn on" the monitoring capabilities for all PIPS and Federal Investigative Services (FIS) related systems.[243] In other words, it took almost eleven days from the time OPM was notified on March 20, 2014 about the data breach for OPM to deploy the capabilities necessary to monitor one of the most high value targets on their IT environment – PIPs.

The US-CERT timeline also highlights other gaps in OPM's information security posture that made OPM vulnerable to attack and put sensitive data OPM held at risk. For example, a March 31, 2014 entry states: "high value, targeted users only needed to authenticate with username and password, which could be compromised remotely – Enforced PIV access for 5 high-value users."[244] Jeff Wagner testified about challenges related to implementing PIV functionality:

> Q. Were they not being enforced prior to that?
>
> A. No.
>
> Q. Why was that?
>
> A. It was a project that was on the list, and to completely change the culture and the functionality of some systems, it takes planning.

---

[241] Wagner Tr. at 19-20.
[242] Saulsbury Tr. at 35.
[243] June 2014 OPM Incident Report at HOGR0818 -001241.
[244] June 2014 OPM Incident Report at HOGR0818 -001242.

Q. When you say the culture of some systems, what do you mean by that?

A. So as users have built systems throughout years or decades, they have become accustomed, and there's business or operational procedures that rely on specific methods. In order to change authentication methods from like user name password to PIV, some of those processes have to get redefined and republished.[245]

Thus, the challenge of fully enforcing multifactor authentication through the use of PIV cards arose in part from the agency's culture. Wagner testified that maintaining the functionality of the production environment was related challenge in deploying PIV. He said: "full deployment of PIV, caused certain applications and certain functionalities to break."[246] Wagner testified that in response to the 2014 breach remediation plan, 100 percent of windows administrators began utilizing PIV cards through an Xceedium appliance,[247] and by September 2014, all OPM users were PIV compliant.[248] According to an OMB Report on Fiscal Year 2014 activities, OPM still had not fully implemented PIV card access rules. OPM was identified in this OMB Report as one of several agencies with the "weakest authentication profile[s]" – meaning a majority of the agency's unprivileged users logged on only with a user ID and password, making an unauthorized access more likely.[249]

While OPM monitored the situation in 2014 to the extent their 2014 security posture allowed, the next step was to develop a remediation plan to eliminate the attackers' presence on the OPM's network. Prior to the May 27, 2014 "Big Bang" effort to eliminate the attackers from OPM's network, OPM began taking other ad hoc measures to mitigate the damage. In early May, OPM began setting up "green zones" —the security team's effort to "eliminate certain administrators from being on the network to be exploited."[250] Wagner described the green zone during his testimony. He stated the green zone was:

---

[245] Wagner Tr. at 38.
[246] *Id.*
[247] Wagner Tr. at 74 (Mr. Wagner testified that, "There is a piece of network equipment that needs to get purchased and installed to finalize the last couple pieces at the Macon site. But to clarify, they're all forced to utilize PIV through the Xceedium Appliance. There just happens to be a potential workaround that we have mitigation pieces in place to prevent.").
[248] Wagner Tr. at 75 (explaining that the exact date that all administrator accounts began PIV compliant varied based upon the location). As of April 2015, OPM reported to OMB that 100 percent of their privileged users were required to use PIV cards and only 41 percent of their unprivileged users were required to use PIV cards. After a 30 day cyber sprint launched in July 2015, OPM reported 97 percent PIV card compliance as of July 2015. Office of Mgmt. & Budget, Exec. Office of the President, *CyberSprint Results* (July 31, 2015) (On file with the Committee).
[249] Office of Mgmt. & Budget, Exec. Office of the President, *Annual Report to Congress: Federal Information Security Management Act* 23 (Feb. 27, 2015) available at: https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy14_fisma_report_02_27_2015.pdf. PIV cards facilitate multifactor authentication credentials to control access. Such technology can at a minimum slow attackers who attempt to use unsecure credentials to move around an IT network. Memorandum from Jacob J. Lew, Dir., Office of Mgmt. & Budget, Exec. Office of the President, to Heads of Exec. Dep'ts. and Agencies, M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12-Policy for a Common Identification Standard for Federal Employees and Contractors* (Feb. 3, 2011), https://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf. .
[250] Wagner Tr. at 137-138.

> [A] creation of independent machines that the database administrators utilizing that was wholly separate from the normal network so that all database access of the database that we knew [the adversaries] were looking for could only be accessed through this one controlled machine, which was not on the network.[251]

Green zone machines were configured at locations in Washington, D.C. and Boyers, Pennsylvania. Deployment and configuration of the green zone workstations continued through May 23, 2014.

Between May 23 and May 27, the US-CERT timeline does not provide a clear description of activities prior to the May 27, 2014 "Big Bang" effort to eliminate the attackers nor provide the reason after two months of monitor May 27 was the designated date.[252] However, testimony given before the Committee does fill in some of this gap. Wagner testified:

> We needed preparation to do the Big Bang. The three-day weekend was coming up. It was something that looked like a perfect time to prestage everything. However, we wanted to ensure that the users were involved and we could get full direct identity of the users when changing passwords. We didn't want to just get a phone call from somebody saying, hey, I need my password changed. We wanted to be able to physically verify that passwords were being changed by users. So that date was specifically chose to prestage all the back-end processes that needed to be in place in order for a full-user reset.[253]

Wagner stated the decision to remove the adversary from the agency's network on May 27 was made as a result of the forensic analysis process and not necessarily related to how close the adversary got to the background investigation system (PIPs). He testified:

> Q. So beyond the period of time to stage the event, were the attackers moving in the network they gave you an indication that you needed to kick them out at this point? Were they getting close to PII? Were they getting close to –
>
> A. It was a point of presence in which the interagency response team felt that there was nothing more to be gleaned from the presence of the adversary. We weren't learning anything new. They weren't searching for anything different. And so the risk of kicking them out too early had come and gone, and now the risk was becoming having them in too long, and we didn't want to keep them around any longer than we had to.[254]

---

[251] Wagner Tr. at 137-138.
[252] June 2014 OPM Incident Report at HOGR0818 -001243.
[253] Wagner Tr. at 39.
[254] Wagner Tr. at 39-40.

Wagner's testimony—that OPM and their interagency partners were no longer gaining useful intelligence from the monitoring phase—is at odds with the testimony of Brendan Saulsbury, an OPM contractor with OPM's IT Security Operations who played a significant role in monitoring the attackers during this period. Saulsbury stated:

> Q. And you and your team were monitoring their penetration. And was there any particular danger that precipitated the decision to conduct the Big Bang when it was conducted?
>
> A. Yes. So we would sort of observe the attacker every day or, you know, every couple of days get on the network and perform various commands. And so we could sort of see what they were looking for. They might take some documentation, come back, and then access, you know, somebody else's file share that might be a little bit closer or have more access into the system. We would sort of see them progress as we are doing our investigation. **And then it got to the point where we observed them load a key logger onto a database administrator's work station, or actually several database administrators' workstations. At that point, the decision was made that they are too close and OPM needs to remove whatever they were aware of at the time.**
>
> Q. Okay. And that precipitated the Big Bang. When you say too close?
>
> A. **They were too close to getting access to the PIPs system.**[255]

The distinction is significant on two levels. First, if Mr. Saulsbury is correct, it is possible that OPM had not yet identified all of the infected systems on their network, i.e. the agency had not yet identified the scope of the hacker's foothold. Second, if the adversary was getting "too close" to the PIPS system it is likely the hacker had conducted sufficient reconnaissance of OPM's network to access that application, but had not yet successfully executed the end-stage of their hack and successfully exfiltrated data.

Regardless of the instigating events, the first phase of the remediation plan (the "Big Bang") was completed on May 27, 2014.[256] OPM took a number of steps in collaboration with US-CERT to "eradicate the malicious actor, at least temporarily, from OPM's network." These steps included: removing all known compromised systems, creating new accounts for 150 known or potentially compromised users and disabling their old accounts, and forcing all Windows administrators to use PIV card for authentication.[257]

---

[255] Saulsbury Tr. at 25-26.
[256] Saulsbury Tr. at 48; Wagner Tr. at 57 (Wagner referring to the end of the monitoring phase as the "Big Bang").
[257] June 2014 OPM Incident Report at HOGR0818-001235.

In addition, the "Big Bang" effort included: resetting administrative accounts; PIV-enforcing all admin accounts; building new accounts for compromised users; resetting all local accounts on all servers; taking the compromised systems off line; and a "stateful" reset of all internet routers.[258] OPM and their interagency partners were effectively attempting to press the reset button and eliminate the adversary's foothold in OPM's environment by eliminating their means of mobility (user accounts) and presence (compromised systems).

OPM continued remediation efforts and was confident the adversary had been removed from their environment. Jeff Wagner, OPM's Director of IT Security Operations testified:

> 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 [redacted] and talk to them to see if there was any communication throughout DHS, FBI, the IC community, if anything that was being identified related to OPM, and there was no communication whatsoever.[259]

Documents and testimony show OPM leveraged both interagency partners and private sector technologies, including Mandiant,[260] to ensure their systems, particularly the PIPS system, were clean of any malicious presence. Saulsbury testified: "The NSA blue team came into OPM and they were performing both vulnerability scans, and scans for malware artifacts on the network."[261]

Wagner and Saulsbury admitted, however, that the attack OPM discovered in 2015 – which led to the exfiltration of background investigation data in the summer of 2014 – was already underway during the 2014 incident response period and continued after the Big Bang.[262] On or about May 7, 2014 and while OPM was closely monitoring the OPM network, the attackers had established a foothold and dropped malware.[263]



[258] June 2014 OPM Incident Report at HOGR0818 -001243.
[259] Wagner Tr. at 40.
[260] Wagner at 54 ("They also deployed some of their technical staff to deploy the Mandiant tool. We didn't have at the time a deployed endpoint search mechanism. So they deployed their Mandiant to our environment to do the search for malware. Actually, there's another component. They also utilized their forensics team to do some of the forensic imaging and then malware analysis once they took the drives -- occasionally took the drives back to DHS headquarters -- DHS office on Glebe to do analysis, forensics analysis.").
[261] Saulsbury Tr. at 27.
[262] Wagner Tr. at 127-128; Saulsbury Tr. at 70-71.
[263] *Id.*

During the 2014 Incident Response Period the Exfiltration of PIPS-related Information Made Clear the Attackers' Target was Background Investigation Data Held in PIPS

During the 2014 incident response period while OPM was monitoring the attackers, OPM observed the exfiltration of data related to the PIPs system. The fact that this information was taken makes clear the target; further, this information likely informed the background investigation data exfiltration that was later discovered in 2015. US-CERT's June 2014 Incident Report Appendix D lists the data exfiltrated while OPM monitored their network in 2014.

Appendix D - Exfiltrated OPM Data

Document Name	Contains PII?
PIPS SAR with CA package April 2008.pdf	No
PIPS.PDF	No
PIPS_PFIS_GFIS Business Processing.DOC	No
EPIC Briefing for CIO v5.ppt	No
EPIC-eQIP only.vsd	No
OPM IAS Modernization Alternatives and Recommendation_v15 81607.doc	No
OPM IAS Business Case_Appendices_v15 81607 - APPENDIX M ONLY2.doc	No
Visio-Phase 1 - Application Creation.pdf	No
Visio-Phase 2 - Application Processing.pdf	No
Visio-Phase 3 - Investigation.pdf	No
Visio-Phase 4 - Case Closing.pdf	No
PIPS IT-Web submission - 9-10-07.pdf.zip	No
PIPS IP Systems & Services on zSeries v3.pdf	No
ZOS Con to Network 02012008.vsd	No
PIPS Data for UPN Match.xlsx	No (Names, Last 4 SSN)
PIPS Fed-Employee List for IT Awareness-2014.txt	No (Names, Last 4 SSN)
PIPS Outside-Agy List for IT Awareness-2014.txt	No (Names, Last 4 SSN)
PIPS Disaster Recovery.url	No
PIPS Programmer Groups.docx	No
pips contractor list 2009.xls	No
PIPS Pgmr Group Access.txt	No
PIPS Pgmr in AP group list.txt	No
PIPS_User Matrix-2-7-2010.xls	No
PIPS-For-UPN.zip	Password Protected (Unable to Open)
PIPS Contractor List for IT Awareness-2014.txt	No (Names, Last 4 SSN, Company)
PIPS EPIC Iteration 1 Dictionary.xls	No
PIPS_Print_Solution_PageCenter.ppt	No
PIPS Batch Job Frequency.xls	No
PIPS-2B-Mapping.xlsx	No
PIPS-R Deletes.xlsx	No
PIPS-R File Usage Data 20090323.xls	No
PIPS_Cluster_Conversion_Plan.xls	No

By way of background, OPM's PIPS is a mainframe application on the OPM environment that stores the background investigation information provided by employees and perspective employees on forms SF-86, SF-85, and SF85P.[264] PIPS interacts with several other

[264] Wagner Tr. at 19; U.S. Office of Pers. Mgmt., *Federal Investigative Service Division Information Technology Privacy Impact Assessment* 43 (Oct. 2006).

Federal Investigative Services (FIS) systems and the connected and component databases contain information and materials that are considered the "crown jewels" for a foreign intelligence service.[265]

Based on the nature of the information held in the PIPS and related systems it was clearly a target, but Jeff Wagner OPM's Director of IT Security Operations seemed to downplay the significant of PIPS as a target. He testified:

> Q. What is the PIP server or system?
>
> A. PIPS is an application that sits on the mainframe.
>
> Q. Why would that be a target for an adversary, that particular application?
>
> A. It's a large data repository.
>
> Q. It's a high-value target?
>
> A. It's currently assessed as a high-value assessment, but it's a large data repository. Any large data repository is always a target.[266]

The PIPs system is more than simply a "large data repository." The data it stores—sensitive background investigation information gathered from SF-86 forms—is some of the government's most valuable PII.[267] Documents that could inform attackers about the nature of and the architecture of PIPS and related systems should not have been permitted to be exfiltrated from OPM's network.

Appendix D (as shown above) lists documents that were exfiltrated during OPM's monitoring effort in 2014. The documents relate to OPM IT systems, including PIPs, contractor information, and documents with names and the last four digits of those individuals' Social Security numbers.[268] Additionally, the documents listed in Appendix D contain information relevant to large repositories of PII information. The list of "Exfiltrated OPM Data" in Appendix D identifies 34 documents.[269] Appendix D indicates none of the documents contained PII (except in one case where the PII was password protected and the adversary was unable to open

---

[265] David Perera & Joseph Marks, *Newly Disclosed Hack Got "Crown Jewels,"* POLITICO, June 12, 2015, available at: http://www.politico.com/story/2015/06/hackers-federal-employees-security-background-checks-118954.

[266] Wagner Tr. at 19.

[267] According to NIST guidance, "PII is —any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information." *See* National Institute for Standards and Technology, Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf.

[268] June 2014 OPM Incident Report Appendix D at HOGR0818 -001245-1246.

[269] *Id.*

it). Four of the documents, however, included the last four digits of individual Social Security numbers.[270]

In describing the items exfiltrated in Appendix D, US-CERT's June 2014 Incident Report makes clear the target was PIPS. The Report stated:

> The attackers primarily focused on utilizing SMB [Server Message Block] commands to **map network file shares of OPM users who had administrator access or were knowledgeable of OPM's PIPs system**. The attackers would create a shopping list of the available documents contained on the network file shares. After reviewing the shopping list of available documents, the attackers would return to copy, compress, and exfiltrate the documents of interest from a compromised OPM system to a C2 server.[271]

Further, there remains the important caveat from US-CERT that additional documents may have been exfiltrated prior to OPM's monitoring phase which began in March 2014. US-CERT stated:

> In should be noted the attackers had **access to OPM's network since July 2012** and the documents [] were exfiltrated during the time period of March 2014 to May 2014 when OPM [] stated their advanced monitoring of the infected systems. **Additional documents may have been exfiltrated prior to March 2014, but there is no way to determine with exact certainty**.[272]

Wagner downplayed the significance of the information exfiltrated in 2014 and testified that the information was "standard" and would not necessarily give an adversary an advantage in a subsequent attack.[273] He testified:

> A. So all of -- so in 2014, the adversary was utilizing a visual basic script to scan all of our unstructured data. So the data comes in two forms. It's either structured, i.e., a database, or unstructured, like file shares or the home drive of your computer, things of that nature. All the data that is listed here, all came out of personal file shares that were stored in the domain storage network. And when I went back to the program offices and had them sit down with us and do an assessment of it and look at the age and the amount of data within these, it was not recognized to be critical data or critical information. It's pretty standard documentation, for the most part.

---

[270] *Id.*
[271] June 2014 OPM Incident Report at HOGR0818 -001234-1235.
[272] June 2014 OPM Incident Report at HOGR0818 -001235.
[273] Notably, OPM produced these documents from Appendix D to the Committee in the Fall of 2015 with redactions and in camera. It was only under subpoena that OPM produced these documents without redactions in February 2016.

Q. When you say "standard documentation," documentation that would be public accessible?

A. I don't necessarily know if it would totally be publicly accessible. I don't know what everyone publishes. But like A&A and C&A packages, for the most part, are available for review; they're traded amongst agencies. It's not something you would be, you know, overly freaked out over.[274]

When questioned further about the significance of the Appendix D documents, Wagner continued to downplay the significance of these documents in his testimony:

Q. One of the entries includes a document that was exfiltrated PIPS contractor list [redacted] Is that the kind of information that you would want in the hands -- not that you would want in the hands of an attacker -- but that would give an attacker an advantage?

A. The list of contractors from 2009 was just simply a user name list of the system. It's not something that's -- it wouldn't necessarily give them an advantage. I mean –

Q. Would knowing the users on a network for a particular system –

A. Finding users is not difficult. For the most part, if you think about it, most companies or agencies utilize a standard-type naming scheme. So it's fairly easy from a pen tester or an adversary standpoint to glean this information, either from initial presence or half the time you can just Google it. For instance, everybody's Facebook account utilizes a Yahoo or a Google email address. It wouldn't be difficult to find anyone, any individual's credentials in some form to figure out what your user name to your Facebook is.[275]

Saulsbury, however, disagreed with Wagner's assessment of the sensitivity of the Appendix D documents that were exfiltrated. He testified that the documents could be useful to the hackers in a subsequent attack. He stated:

Q. So tell me first of all, are these public things that OPM would be concerned about if they were put out into the open?

A. Yes, these are not documents that are meant to be public.

Q. And what kind of documents are these if you could generally characterize them?

---

[274] Wagner Tr. at 41.
[275] Wagner Tr. at 42.

A. They are basically, sort of system documentation, various processes, and related to the background investigation systems.

Q. So if an attacker were able to exfiltrate this type of data, which it appears they did, would this give them an advantage for a future attack?

A. Yes.

Q. And how so?

A. **It gives them more familiarity with how the systems are architected. Potentially some of these documents may contain accounts, account names, or machine names, or IP addresses, that are relevant to these critical systems.**[276]

Saulsbury's testimony indicates the exfiltrated documents in Appendix D contained information relevant to understanding "how the system works." These documents included among other things a 2014 list of contractors with access to the PIPS system, a CIO-level briefing on the EPIC system and a discussion of the interface between the PIPS and Joint Personnel Adjudication System (JPAS) systems. These documents would have improved an adversary's understanding of OPM's system, its architecture, and information on who has access to the background investigation information contained on the PIPS system. The Appendix D information is significant because it would be useful to an attacker and it provides further evidence that the hackers were targeting PIPs. Nonetheless, Mr. Wagner's characterization seems to downplay the significance of the Appendix D.

Given the near certainty that PIPS and the information it held was a target before and confirmed during the 2014 incident response period, it is noteworthy that OPM's network monitoring technology did not have total visibility into PIPS. Wagner testified, "I guess it would be fair to say that there was minimum visibility of the PIPS application itself."[277] Despite this lack of visibility, OPM asserted they were confident no PII was taken during the course of the 2014 data breach. Wagner testified:

Q. Without monitoring tools on the PIP server at that point, at least insofar as this is described, could data from the PIPS application have been taken prior to March 28th and OPM had not been aware of that?

A. That would not be possible.

Q. Why is that?

---

[276] Saulsbury Tr. at 27-28.
[277] Wagner Tr. at 20.

A. Because it would have to pass through the distributing environment to do so. The mainframe sits within the center of the distributed nucleus, so in order to get data out, it would have to pass through all the other monitoring techniques.

Q. And why would that allow you to see it?

A. Because we had seen large sums of data leaving.

Q. And that would be –

A. -- we've seen large spikes and things of that nature, and DHS and us, both, looked for those large spikes at that time, and we did not see any.[278]

OPM has consistently asserted that no PII data was taken in the 2014 breach, but as US-CERT stated "additional documents may have been exfiltrated prior to March 2014, but there is no way to determine with exact certainty.[279] At a minimum sensitive data was in fact exfiltrated by the hackers, as evidenced by the items listed in Appendix D. The Appendix D data exfiltrated provided clues as the data targeted and the tactics, techniques and procedures (TTPs) of the attackers OPM monitored in 2014 provided hints about the data breach OPM later discovered in 2015.

Tactics Techniques & Procedures (TTPs) of Attackers Discovered in 2014: Hikit Malware and SMB Protocol

The attackers discovered in 2014 used Tactics, Techniques & Procedures (TTPs) —such as the type of malware and the attackers' ability to move throughout OPM's network—hinted at the targets of the attack OPM discovered in 2015. These TTPs also indicate the persistence, scope, and sophistication of attacks on OPM's network. Those key pieces of information, however, were not enough for OPM to stop the far more serious attack discovered in 2015. A public report by a threat analysis group has said the attackers discovered in 2014 used a specific and uncommon toolkit—or malware—designed for late-stage persistence and data exfiltration.[280]

The malware used by the attackers discovered in 2014 was identified as two variants of HiKit malware, referred to as HiKit A and HiKit B.[281] Notably, an October 2014 FBI Cyber Flash Alert said HiKit malware should be "given the highest priority for enhanced mitigation," and it "uses rootkit functionality to sit between the network interface card and the operating system enabling the malware to sniff all traffic to/from the compromised host."[282]

---

[278] Wagner Tr. at 20.
[279] June 2014 OPM Incident Report at HOGR0818 -001235.
[280] Novetta, *Operation SMN: Axiom Threat Actor Group Report* at 6.
[281] Saulsbury Tr. at 17; June 2014 OPM Incident Report Appendix C at HOGR0818-001244 - 1245.
[282] Cyber Div., Fed. Bureau of Investigation, A-000042-MW, *FBI Cyber Flash Alert* (Oct. 15, 2014), http://www.slideshare.net/ragebeast/infragard-hikitflash.

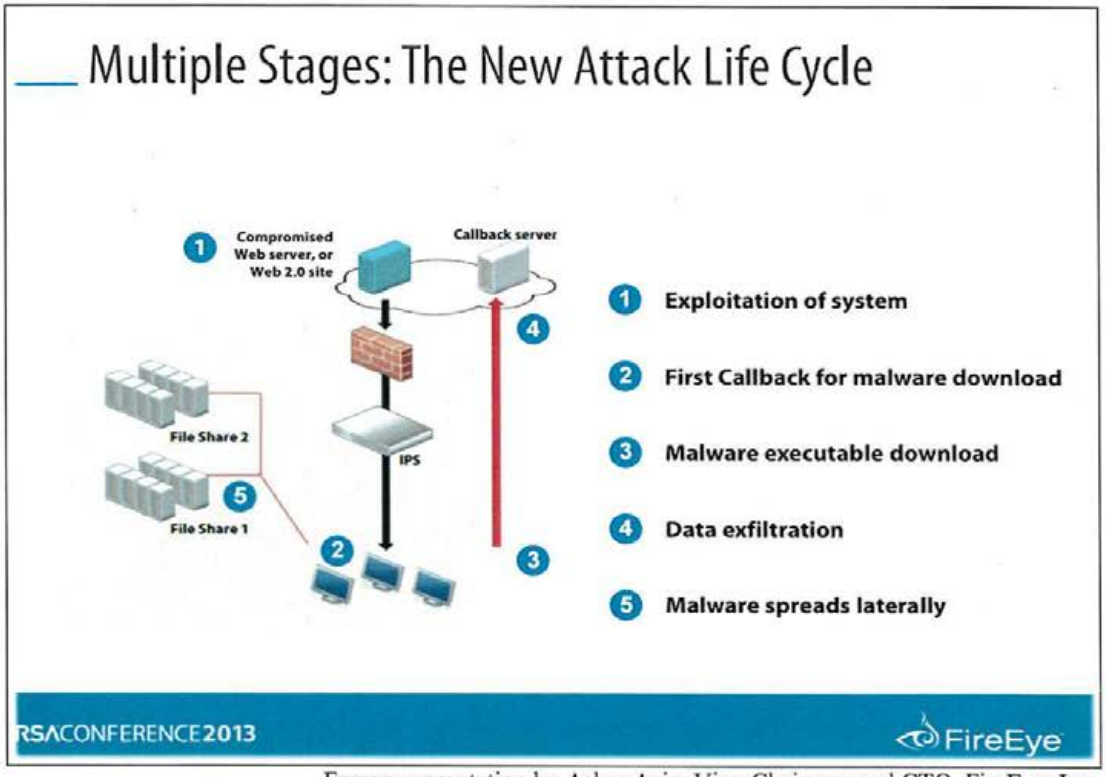
The use of HiKit malware is evidence of a sophisticated attacker that had achieved persistence on the IT environment, and was capable of performing a variety of functions (including data exfiltration) within OPM's network. In the 2014 Incident Report, US-CERT described Hikit as an "extremely stealthy form of malware designed to hide its malicious processes and programs from detection of commodity intrusion detection and anti-virus products."[283] Saulsbury described how the HiKit malware was used by the attackers discovered in 2014. He testified:

> So the fact that it is still beaconing means that an attacker could use it to still obtain entry into OPM's network. It just means that they could get onto that command and control server and start issuing commands to that infected machine. So C2 means command and control. As far as it being an IP rather a domain, that's not a significant issue. Basically, the way that their malware worked was there is a configuration file that tells the malware where to beacon out to. And instead of it having a domain that they created, they just put the IP directly in there, so instead of doing DNS resolution it just goes directly out, so it is just a quirk.[284]

Wagner described Hikit as a "form of a remote access tool, or RAC. It's a, basically, a back-door command tool," with "multiple functionalities. Most malware these days are kind of a Swiss Army knife type effect. You don't necessarily have a functionality like key logger. It usually utilizes multiple modules that allow various activities."[285] Wagner also said the Hikit malware was mostly used for persistence, or maintaining a presence at OPM, though keylogging activity was also observed.[286] Effectively, the malware was used so the hackers could "still use it to obtain entry into OPM's network."[287]

---

[283] June 2014 OPM Incident Report at HOGR0818 -001234.
[284] Saulsbury Tr. at 18-19.
[285] Wagner Tr. at 31.
[286] Wagner Tr. at 18.
[287] Saulsbury Tr. at 18.



From a presentation by Ashar Aziz, Vice-Chairman and CTO, FireEye, Inc. at RSA Conference USA 2013 (Feb. 28, 2013)

In other words, the Hikit malware is a rootkit—or a set of software tools that allow an unauthorized user to gain control of a computer system, escalate access, and persist in presence on the network without being detected. US-CERT explained that Hikit allowed the hackers to gain root level or administrator access to OPM's network and:

> [A]llow[ed] the attackers to create a reverse shell from their C2 [command and control] servers into the infected systems in OPM's network from a remote location anywhere in the world. The C2 servers are used to proxy the attackers' connections from their actual location on the Internet in order to keep their real identities and locations hidden. Hikit allows the attacker to run commands and perform functions from a remote location as if they had the equivalent of a monitor and keyboard connected to the compromised OPM system.[288]

The presence of Hikit on the OPM network was evidence of the adversary's presence and capabilities, but it did not reveal the initial point of entry. However, the use of a rootkit means the attackers had to have high level access to OPM's network. US-CERT said, the attacker was able to acquire high level credentials by exploit a vulnerability and likely obtained access to OPM's network using social engineering methods, such a phishing attack.[289] Outside threat analysis experts have described Hikit as a "late-stage persistence and data exfiltration tool" that

[288] June 2014 OPM Incident Report at HOGR0818 -001234.
[289] *Id.*

indicates the final phases of the threat actor's operational lifecycle.[290] The use of Hikit is evidence of a multistage operational lifecycle that would require the adversary to not only be well resourced, but also well organized.[291] The attack discovered in 2015 had similar characteristics.

The Hikit malware allowed the attackers to remain on OPM's systems—to maintain persistence—but in order to move throughout OPM's network undetected, the attackers used Server Message Block (SMB) protocols.[292] Hikit and SMB protocols are TTPs that tend to suggest "advanced penetration" and a sophisticated actor.[293]

With respect to the use of the SMB protocols, US-CERT said, "the malicious actors were connecting into the [redacted] server between the hours of 10pm and 10am EST with a compromised Windows domain administrator credential to search for PIPs related files on OPM's network file servers utilizing SMB commands."[294] Wagner described the attackers' use of SMB protocols during the 2014 attack. He testified:

> If you do some form of traversal or communications, you run over a normal communications protocol. It's not uncommon to change the protocol language or change the protocol ports in which you do traffic. And essentially, what they did is they tried to hide their activity and the things they were doing in a very highly utilized protocol port. So they basically hid their communications in the fuzz of the [network] traffic.[295]

Wagner acknowledged that the use of SMB protocols, in addition to other TTPs, were evidence of the threat actor's sophistication and capabilities. Wagner testified:

> Malware itself doesn't indicate sophistication. The other tactics and techniques that they utilized, or other things that they did, such as hiding their commands through, SMB, shows an advanced penetration. It's not a simple attack.[296]

The use of the Hikit malware and SMB protocols by the attackers discovered in 2014 show the attackers had a well-developed foothold in OPM's environment – and maintained a presence and persistence that indicated an advanced penetration that OPM was facing in 2014. NIST described the challenge of a persistent late stage penetration:

> [U]nderstanding threats and identifying modern attacks in their early stages is key to preventing subsequent compromises . . . preventing problems is often less costly and more effective than reacting to them after they occur. Thus, incident prevention is an important complement to an

---

[290] Novetta, *Operation SMN: Axiom Threat Actor Group Report* at 6.
[291] *Id.*
[292] June 2014 OPM Incident Report at HOGR0818 -001231.
[293] Wagner Tr. at 33.
[294] June 2014 OPM Incident Report at HOGR0818 -001233.
[295] Wagner Tr. at 16.
[296] Wagner Tr. at 31.

incident response capability. If security controls are insufficient, high volumes of incidents may occur.[297]

OPM's Network Logging Capabilities Limited Investigating the "How" and "How Long" for Attackers Discovered in 2014

OPM's ability to determine the "how" and "how long" of the attackers discovered in 2014 was limited by significant gaps in their capability to create, collect, and review audit logs of their network. Consequently, the answers to these questions remain unclear.

Audit logs are collections of events that take place on information technology systems and networks.[298] In the course of a forensic investigation, a variety of sources produce reviewable log information, including: antivirus software, firewalls, and intrusion detection and prevention systems.[299] These sources can help investigators piece together how the attacker gained access, where the attacker has been, how long they have been there, and, most importantly, give clues as to what the attackers are after.[300]

US-CERT identified numerous gaps in the centralized logging of security events at OPM during the investigation of the attackers discovered in 2014 stating: "Currently, OPM utilizes Arcsight as their SIEM [security information and event management] solution of choice, but there are numerous gaps in auditable events being forwarded to Arcsight for analysis, correlation, and retention."[301]

Gaps in OPM's audit logging capability likely limited OPM's ability to answer important forensic and threat assessment questions related to the incident discovered in 2014. This limited capability also undermined OPM's ability to timely detect the data breaches that were eventually announced in June and July 2015.[302] If IT security teams can track the attackers' movements back to the point of entry, they can patch the system vulnerabilities that allowed the penetration in the first place.

The OPM team did not, at the time of the incident discovered in 2014, have a robust logging capability that would have allowed them to determine the initial point of entry. Wagner acknowledged the audit logging gap and how that impacted their ability to identify the initial

---

[297] Paul Cichonski et. al., Nat'l Inst. of Standards & Tech., Spec. Pub. 800-61rev. 2, *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology* 2 (Aug. 2012), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

[298] *See generally* Karen Kent & Murugiah Souppaya, Nat'l Inst. of Standards and Tech., Sp. Pub. 800-92, *Guide to Computer Security Log Management* (2006).

[299] *Id.*; *see also* Saulsbury Tr. at 15 (testifying that "There are many different log sources that we look at during a forensic investigation.").

[300] *E.g.* Wagner Tr. at 17-18; Saulsbury Tr. at 27.

[301] June 2014 OPM Incident Report at HOGR0818-001237.

[302] U.S. Office of Pers. Mgmt., Press Release, *OPM to Notify Employees of Cybersecurity Incident* (June 4, 2015), https://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident/; U.S. Office of Pers. Mgmt., Press Release, *OPM Announces Steps to Protect Federal Workers and Others from Cyber Threats* (July 9, 2015), https://www.opm.gov/news/releases/2015/07/opm-announces-steps-to-protect-federal-workers-and-others-from-cyber-threats/.

point of entry. He stated: "I don't think we ever necessarily found initial point of presence or point of contact. Our last log entries at best, gave us the evidence of adversary presence, was November of 2013."[303] Wagner also testified:

> We did forensics to try to find the initial point of infection, but because we didn't have the full volume of logging that we have today throughout 2013 or 2012, or prior to the 2014 breach, we just ran into a point where there wasn't logs to give us sufficient evidence or indication of the exact point of presence.[304]

Saulsbury also acknowledged the limited logging capability. He stated:

> Q. Okay. And after all was said and done and you were looking back, when were the earliest actions taken by the hackers relating to the breach? And when did they take place? And what were they?
>
> A. So we don't know with 100 percent certainty what the initial entry point into the network was and when it was. So what we were able to do is look back through some of the logs that we had and try to find -- I can't remember at this point what the actual -- like our earliest log entry of activity was. I want to say that we had stuff, activity at least back in 2013 that was observed, but I can't recall at this point what the first evidence that we have is.[305]

The gaps in audit logs not only make it difficult to determine how the attackers perpetrated their hack of OPM, but also to determine with any degree of certainty how long the attackers were in the OPM network and any data exfiltrated. US-CERT said of the attackers discovered in 2014:

> It should be noted that the attackers had access to OPM's network since July 2012 and the documents below were exfiltrated during the time period of March 2014 and May 2014 when OPM CIRT started their advanced monitoring of the infected systems. Additional documents may have been exfiltrated prior to March 2014, **but there is no way to determine with exact certainty**.[306]

OPM also could not accurately assess the risks to their IT environment because the agency lacked the necessary logging information and centralization practices to generate a full picture of how the hackers established and then maintained persistence on OPM's systems. Threat and vulnerability information are the foundational step in implementing NIST's risk-based approach.[307]

---

[303] Wagner Tr. at 17-18.
[304] Wagner Tr. at 27.
[305] Saulsbury Tr. at 14-15.
[306] June 2014 OPM Incident Report at HOGR0818-001235.
[307] Comput. Sec. Div., Nat'l Inst. of Standards and Tech., *Risk Management Framework (RMF) Overview* (last updated Apr. 1, 2014), http://csrc.nist.gov/groups/SMA/fisma/framework.html.

The agency's inability to determine what other documents were exfiltrated prior to March 20, 2014 revealed two flaws in OPM's network monitoring practices. First, from March 2014 forward, US-CERT and OPM were installing the monitoring equipment, including additional logging capabilities, to determine what was being exfiltrated going forward. This left the agency with limited ability to look backwards. Second, the gaps in OPM's monitoring practices prevented OPM from determining what exactly was leaving the network and what data had been taken in the nearly two years the attackers had access to OPM's network.

After investigating the attackers discovered in 2014, US-CERT recommended OPM implement a robust system audit log data practice and:

> Require program offices to send critical system audit log data to Arcsight. During the system development life cycle, security related information and auditing requirements should be identified in accordance with OPM IT Security Policy and NIST recommended guidelines and configured to be sent to Arcsight for analysis, correlation, and retention. The following log sources were identified by Network Security as a high priority: Linux Secure Logs, HRTI Active Directory Logs, RACF authentication logs, and PIPS access logs. Aggregation of audit log data to centralized location such as Arcsight allows for proactive security monitoring and quicker time for triaging and remediating security incidents. (Low level of effort to implement).[308]

Wagner testified that OPM now (as of February 2016) has 100 percent visibility over their systems, but it is not clear when OPM gained this increased visibility. He stated:

> Q. Did you have total visibility over OPM's environment during the 2014 incident?
>
> A. I would not say 100 percent. We had a great deal of visibility. Actually, at the time, we had full visibility on the perimeter. Internal visibility, is where we had some gaps.
>
> Q. Why is that?
>
> A. As I said, it was an issue in which there was a longstanding project to have long entries loaded into the logger. Post the 2014 incident, that became a major priority, and we now have 100 percent visibility.[309]

It is notable that as Mr. Wagner admits they may have had significant visibility on the perimeter of the OPM network, but the gaps were more pronounced once the attacker was already inside the perimeter. Thus, an attacker already inside seemed to have the ability to move

[308] June 2014 OPM Incident Report at HOGR0818 -001237.
[309] Wagner Tr. at 33.

undetected across OPM's network. In a zero trust environment, an attacker's ability move once inside a network environment would be limited by a segmented environment and strong access controls.

As noted earlier, the attacker later discovered in 2015, had already established a foothold inside the OPM network as of early May 2014.

Chapter 3: OPM Attempts to Mitigate the Security Gaps Identified in 2014 While Iron Man and Captain America Go to Work (May 2014 – April 2015)

After the "Big Bang" effort on May 27, 2014, there were a number of events that inform the story of the data breaches announced in 2015. These events are also relevant to April 15, 2015—when OPM first identified an unknown SSL certificate[310] used to communicate with, an at the time, unknown domain: "opmsecurity.org."[311] "Opmsecurity.org" was later found to be registered to Steve Rogers—Captain America's alter ego. OPM subsequently identified another domain, "opmlearning.org," which was registered to Tony Stark—Iron Man's alter ego. These domains were part of an advanced and sophisticated attack infrastructure used to exfiltrate data from OPM in the summer of 2014.

As OPM and a multi-agency team began to investigate the scope and method of the attack, OPM enlisted the assistance of two contractors, Cylance and CyTech. The multi-agency team and contractors eventually made findings that caused OPM to announce in June and July 2015 that the personnel records for over 4 million individuals and background investigation data for over 20 million individuals had been compromised.[312]

To fully appreciate the May 2014 through April 2015 period, it is useful to establish OPM's posture with respect to mitigating the threat of the cyber incident that was identified in March 2014.

OPM's IT Security Posture and Mitigation Efforts After the May 2014 "Big Bang"

On June 22, 2014, US-CERT issued an Incident Report to OPM with fourteen observations and recommendations to address the security gaps identified in the aftermath of the 2014 cyber incident. The observations and recommendations in this Report highlighted the poor state of IT security at OPM and the failure to implement basic cyber hygiene practices.

The Incident Report directed OPM to "redesign their network architecture to incorporate security best practices."[313] Brendan Saulsbury, an OPM contractor who participated in OPM's 2014 and 2015 incident response efforts testified that US-CERT deemed OPM's network "**very insecure, insecurely architected" and found there was "lots of legacy infrastructure.**"[314]

---

[310] An SSL is a security sockets layer and is standard security technology used to establish an encrypted link between a server and a website.

[311] June 9, 2015 DMAR at HOGR0724-001154.

[312] U.S. Office of Pers. Mgmt., Press Release, *OPM to Notify Employees of Cybersecurity Incident* (June 4, 2015), https://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident/; U.S. Office of Pers. Mgmt., Press Release, *OPM Announces Steps to Protect Federal Workers and Others From Cyber Threats* (July 9, 2015), https://www.opm.gov/news/releases/2015/07/opm-announces-steps-to-protect-federal-workers-and-others-from-cyber-threats/.

[313] June 2014 OPM Incident Report at HOGR0818-001235.

[314] Saulsbury Tr. at 16-17.

Saulsbury said this ultimately led to OPM's decision to "create basically a brand new hardened network" they called "the shell."[315] According to Saulsbury, OPM intended to eventually move legacy applications to the new shell.[316] US-CERT's 2014 Incident Report identified several specific technical recommendations to improve OPM's network security in the legacy environment, including buying security tools and reorganizing the OCIO.[317]

The US-CERT Incident Report included the level of effort required from OPM to implement each recommendation, from low to high. Three recommendations were considered "low" effort, four "moderate," and two "high."[318]

The US-CERT Incident Report found OPM did not have the capability to centrally manage and audit firewall access control lists and rules. Consequently, DHS recommended short and long term actions to combine manual auditing and scanning tools and then buy a network equipment solution to centrally manage configuration settings while also auditing these settings against best practices. This recommendation was considered "high level of effort."[319]

The Report also found OPM's network was **"extremely flat" and had "little to no segmentation**."[320] Thus, US-CERT recommended a redesign of network architecture with security best practices incorporated, including enforcing no direct user access to servers and requiring PIV credentials for access in order **to "limit an attacker's ability to move laterally across the network once initial access is obtained**."[321] This was a "high level of effort" recommendation.

The recommendations that required a low level of effort to implement were related to logging, security awareness training, and a redesign of OPM's Incident Response Plan.

In recommendations related to the OCIO, US-CERT found "**there is a gap in information technology leadership across OPM as an agency**" and that "**it is not uncommon for existing policies to be circumvented in order to achieve business functions while exposing the entire agency to unnecessary risk.**"[322] In response, US-CERT recommended OPM undertake a policy review and gap analysis to determine the need for additional policies to manage IT security and business functions and noted a "cultural change will need to occur to ensure policies are never circumvented unless absolutely required."[323] DHS also recommended

---

[315] Saulsbury Tr. at 16-17.
[316] *Id.*
[317] June 2014 OPM Incident Report at HOGR0818-001235. *See also* OPM Cybersecurity Events Timeline. The OPM Cybersecurity Events Timeline states that the OPM Security Operations Center (SOC) began unofficially reporting to the OPM CIO in April 2014, and officially began reporting to the OPM CIO in March 2015 after the union approved the reorganization. As of March 22, 2015, the relevant unions at OPM formally approved the OCIO reorganization.
[318] June 2014 OPM Incident Report at HOGR0818-001236 -39.
[319] June 2014 OPM Incident Report at HOGR0818-001236.
[320] *Id.*
[321] *Id.*
[322] June 2014 OPM Incident Report at HOGR0818-001238.
[323] *Id.*

reorganizing the OCIO.[324] Among other things, the reorganization shifted the Director of Security Operations to report to the CIO.[325]

Documents and testimony show OPM began to implement the DHS recommendations in or around May or early June of 2014. The effort continued through early 2016. Based on testimony from two witnesses involved in responding to the 2014 incident, it appears OPM tried to implement DHS's recommendations, but the agency was hindered by the fact that it started with a woefully unsecure network. Throughout this phase, the attackers involved in the data breaches announced in 2015 had already established a foothold on the OPM network.[326]

Key 2014 US-CERT Recommendations Highlighted OPM IT Security Vulnerabilities

One of DHS's key recommendations was to ensure all OPM users were required to use PIV cards for access to the OPM network.[327] In a 2015 OMB Report on IT security, OPM was identified at the end of fiscal year 2014 as one of several agencies with the "weakest authentication profile[s]"—meaning a majority of the agency's unprivileged users logged on only with a user ID and password, making an unauthorized access more likely.[328] The OMB Report also stated that at OPM, only one percent of user accounts required PIV cards for access.[329] Wagner, Director of IT Security Operations stated PIV card enforcement did not fully roll out until September 2014, and was being implemented through early 2015.[330] He added the FIS [Federal Investigative Services] contractors (who did the background investigations) were the last group required to have PIV cards for access.[331]

Had OPM leaders fully implemented the PIV card requirement – or two-factor authentication – security controls when they first learned hackers were targeting background investigation data, they could have significantly delayed or mitigated the data breach discovered in 2015. The agency first learned attackers were targeting background investigation data on

---

[324] June 2014 OPM Incident Report at HOGR0818-001238.
[325] OPM Cybersecurity Events Timeline.
[326] Wagner Tr. at 75-78 (discussing implementation status of two recommendations); Saulsbury Tr. at 31-34 (discussing implementation status of six recommendations and noting logging capability gaps remain due to technical difficulties applying the logging function to mainframes); June 9, 2015 DMAR at HOGR0724-001154.
[327] In August 2004, the federal government initiated several initiatives to enhance cybersecurity across the federal government, including Homeland Security Presidential Directive 12 (HSPD-12). HSPD-12 established a mandatory government-wide standard for secure and reliable identification for access to government IT systems and facilities that was further defined as a requirement for personal identity verification (PIV) credentials. Then OMB directed federal agencies to issue and use PIV cards to control access. OMB reported that as of the end of fiscal year 2014, only 41 percent of all agency user accounts at the CFO Act agencies required PIV cards to access agency IT systems.
Cyber Threats and Data Breaches Illustrate Need for Stronger Controls Across Federal Agencies: Hearing Before Subcomm. on Research & Tech. and Subcomm. on Oversight of the H. Comm. on Science, Space & Tech., 114th Cong. (July 8, 2015) (testimony Gregory C. Wilshusen, Dir. of Info. Sec. Issues Gov't Accountability Office).
[328] Office of Mgmt. & Budget, Exec. Office of the President, *FY 2014 Annual Report to Congress: Federal Information Security Management Act* at 23 (Feb. 27, 2015) available at: https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy14_fisma_report_02_27_2015.pdf.
[329] *Id.* at 20.
[330] Wagner Tr. at 38, 75.
[331] Wagner Tr. at 75.

March 20, 2014.[332] Yet the first data major exfiltration — involving 21.5 million individuals' background investigation files — did not occur until early July 2014, giving the agency over three months to implement security controls to protect those data.[333] Testimony from the Department of Homeland Security revealed that OPM's implementation of two-factor authentication for remote logons in January, 2015 — which was already required of federal agencies — "stopped the adversary from taking further significant action."[334] If OPM leadership had implemented two factor authentication even earlier, for example in April or May of 2014, the agency might have locked out attackers before they had a chance to commit the most significant digital violation of national security faced to date.

In July 2015, OMB launched a "cybersprint" to require all agencies to expedite implementation of cybersecurity measures, including enforcement of PIV card access, within 30 days. According to OPM, 100 percent of their privileged users were required to use PIV cards as of April 2015, but only 41 percent of their unprivileged users were required to use PIV cards. The agency improved its PIV card compliance—by July, 97 percent of unprivileged users were required to use PIV cards.[335]

In August 2015, OPM updated its PIV card implementation status in response a request from the Committee. The agency reported "approximately 99 percent of OPM users are required to use a PIV card (or equivalent) to access OPM workstations with two-factor authentication."[336] The agency also told the Committee that OPM bought 5,000 ActivClient licenses in 2009 to enable the use of PIV card credentials to access OPM workstations and further clarified that currently 8,400 such licenses "are activated, current, and operational."[337] The agency's response raised questions as to the status of the 5,000 licenses purchased in 2009 and why PIV card enforcement was not a priority earlier, particularly given that OMB had identified OPM as an agency with one of the "weakest authentication profile[s]."[338] The use of basic cyber hygiene practices, such as full implementation and enforcement of PIV card access, would have limited the damage incurred during the 2015 data breach incidents.

---

[332] Dep't of Homeland Security/US-CERT and OPM, OPM Cybersecurity Events Timeline (Aug. 26, 2015) (OPM Production: May 13, 2016).
[333] *Id.*
[334] *Under Attack: Federal Cybersecurity and the OPM Data Breach: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 114th Cong. (2015) (statement of Andy Ozment, Assistant Secretary for Cybersecurity & Communications, Department of Homeland Security) (adversary activity June 2014 to January 2015, stopped by security control rolled out January 2015); *see* Dep't of Homeland Security/US-CERT and OPM, OPM Cybersecurity Events Timeline (Aug. 26, 2015) (OPM Production: May 13, 2016) (security control rolled out January 2015 was two factor authentication for remote access).
[335] Office of Mgmt. & Budget, Exec. Office of the President, *CyberSprint Results* (July 31, 2015) (On file with the Committee).
[336] Letter from Jason Levine, Dir. Congressional, Legislative & Intergovernmental Affairs, U.S. Office of Pers. Mgmt., to the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform (Aug. 28, 2015).
[337] *Id.*
[338] Office of Mgmt. & Budget, Exec. Office of the President, *FY 2014Annual Report to Congress: Federal Information Security Management Act* 23 (Feb. 27, 2015) available at: https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy14_fisma_report_02_27_2015.pdf..

OPM Efforts to Buy Security Tools to Secure the Legacy Network and Rebuild OPM's "Very Insecure, Insecurely Architected Network"

In response to US-CERT observations and recommendations in the 2014 Incident Report, OPM launched a multi-phase IT Infrastructure improvement project to (1) buy security tools to secure their legacy network and (2) create an entirely new network environment.

Former OPM CIO Donna Seymour testified to the Committee this project began after the March 2014 cyber incident.[339] In May 2014, Seymour contacted Imperatis, an IT security contractor, to discuss the project. In an email to former colleagues at Imperatis, Seymour wrote: "[D]o you recall all the work we did at MARAD [U.S. Maritime Administration] to straighten out a very messy network with poor security? Well . . . I'm looking for an expert consultant who can guide me and my team through the exact same thing."[340] Seymour and two Imperatis employees worked together at MARAD.[341]

Ultimately, these discussions led to a sole source contract award to Imperatis for the multi-phased IT Improvement project, in June 2014.[342] The project included four phases:

(1) Tactical (securing the legacy IT environment).

(2) Shell (creating a new data center and IT architecture).

(3) Migration (migrating all legacy IT to the new architecture).

(4) Cleanup (decommissioning legacy hardware and systems).

Phase 1, or the Tactical phase, supported OPM's effort to buy security tools to secure the agency's legacy IT environment immediately following the 2014 incident. The Tactical phase of the project began in June 2014 and was completed in September 2015.[343]

OPM's efforts to buy security tools involved interactions with a number of contractors, including Cylance and CyTech which would later provide cybersecurity and forensic solutions to

---

[339] *OPM Data Breach: Hearing Before the H. Comm. On Oversight and Gov't Reform*, 114th Cong. (June 16, 2015) (testimony of Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt.).

[340] Email from Donna Seymour, Chief Info Officer, U.S. Office of Pers. Mgmt., to Patrick Mulvaney and [redacted] Imperatis (May 10, 2014, 9:46 a.m.), Attach. 12 at 001463 (Imperatis Production: Sept. 1, 2015).

[341] *Id.*; Imperatis Proposal Volume II – Staffing and Management, Attach. 5a at 262-264, 268-270 (Appx. A: Key Personnel Resumes), (Imperatis Production: Sept. 1, 2015).

[342] Imperatis Letter Contract (June 16, 2014), Attach. 1 at 000003 (Imperatis Production: Sept. 1, 2015). The OPM OIG raised concerns about the sole source nature of this contract but did acknowledge given the urgency need to secure the OPM legacy network making a sole source award for purposes of buying security tools (Tactical phase) was reasonable. U.S. Office of Pers. Mgmt., Report No. 41-CI-00-15-055, *Flash Audit Alert – U.S. Office of Personnel Management Infrastructure Improvement* Project 5 (June 17, 2015) [hereinafter OIG Flash Audit Alert (June 17, 2015)].

[343] Letter from Imperatis to H. Comm. on Oversight & Gov't Reform Majority Staff (Feb. 12, 2016) (on file with the Committee).

OPM.[344] Documents and testimony show Cylance began conversations with OPM about their products through a reseller, and CyTech was introduced to OPM through Imperatis.

The Committee obtained documents that show OPM was buying and deploying at least ten security tools to the legacy IT environment. Websense is one such tool. In 2014, Websense had limited functionality and simply filtered users' web traffic to prevent access to certain sites (like gambling sites).[345] The agency had to upgrade Websense because, according to Saulsbury, the old version "wasn't performing" and did not include the "advanced capabilities" such as web filtering, email and data security functionality.[346] Saulsbury also testified that in 2014, the Websense server was not the primary target.[347] Saulsbury believed the Personnel Investigations Processing System (PIPs) was the target.[348]

The Websense upgrade was identified as a Priority 1 task and OPM quickly made a purchase in June 2014, but the phased deployment of this tool was not completed until September 2015.[349] As of February 2015, there were continuing challenges with the Websense pilot and as of April 2015 the project status for Websense was only at about 60 percent complete.[350] Saulsbury testified one of the deployment challenges was balancing "usability and security," but, after the 2014 incident, there was less resistance from users and security became the higher priority.[351] In April 2015, according to OPM, the first indicators of compromise were detected (including the unknown SSL certificate that was beaconing to the domain "opmsecurity.org") during the roll out of the upgraded version of Websense.[352]

The agency purchased another tool to improve network access control: [redacted][353] The agency purchased [redacted] on July 28, 2014, and deployed it from September 2014 - September 2015.[354] Documents show the [redacted] deployment was delayed at least in part by required notifications to relevant unions. In August 2015, an Imperatis Weekly Report stated that "project sponsor [for [redacted]] is in notification stage with the Union" and the proposed mitigation strategy to "prepare updated project timeline, plan & memo to pilot [redacted] to non-Union Agency users.[355]

In the aftermath of the 2014 incident, OPM attempted to implement DHS's recommendations, including buying new security tools and building a new IT environment, but

---

[344] *See Infra* Chapters 4, The Role of Cylance and Chapter 5, The CyTech Story.
[345] Saulsbury Tr. at 17-18.
[346] Saulsbury Tr. at 49.
[347] Saulsbury Tr. at 17-18.
[348] *Id.*
[349] OPM Tactical Toolset: Purchase, Kick-off and Completion Timeframes (Oct. 21, 2015) (Imperatis Production: Oct. 21, 2015); Saulsbury Tr. at 50.
[350] Imperatis Weekly Report (Apr. 13, 2015-Apr. 17, 2015), Attach. 6 at 000737 (Imperatis Production: Sept. 1, 2015); Imperatis Weekly Report (Apr. 20, 2015-Apr. 24, 2015), Attach. 6 at 000753 (Imperatis Production: Sept. 1, 2015).
[351] Saulsbury Tr. at 53.
[352] Saulsbury Tr. at 58-59.
[353] Imperatis Monthly Program Review (July-Aug. 2014), Attach. 7 at 000973 (Imperatis Production: Sept. 1, 2015).
[354] OPM Tactical Toolset: Purchase, Kick-off and Completion Timeframes (Oct. 21, 2015) (Imperatis Production: Oct. 21, 2015).
[355] Imperatis Weekly Report (Aug. 3, 2015-Aug. 7, 2015), Attach. 6 at 000942 (Imperatis Production: Sept. 1, 2015).

because of the state of IT security at OPM was so poor, there was much to do. The agency, however, missed opportunities to prioritize the purchase and deployment of certain cutting edge tools that, as Cylance CEO Stuart McClure testified, "would have prevented this attack."[356] Meanwhile, as OPM worked to deploy badly needed security tools, Captain America and Iron Man were exfiltrating sensitive data from OPM's unsecure IT environment in the summer of 2014.

OPM Missed Key Developments

The Committee obtained evidence that shows OPM was working to respond to the attackers discovered in the spring through the summer of 2014, while the attacker groups who ultimately stole background investigation and personnel records data were moving through the agency's network. OPM did not discover the attackers responsible for the background investigation data breach – until April 2015 when it was too late. These attackers had already established a foothold in OPM's network as of early May 2014 and began to exfiltrate this data in early July 2014. Meanwhile, OPM continued its mitigation efforts in response to the attackers discovered in 2014. Documents and testimony show a timeline of key events that provide context for data breach discoveries made beginning in April 2015:

- **July 2012** – Attackers had access to OPM's network.[357]
- **November 2013** – The first known adversarial activity begins in OPM's network that led to the breach identified by US-CERT in March 2014.[358]
- **December 2013 –** Adversarial activity to harvest credentials from OPM contractors begins by the attackers later identified in April 2015.
- **March 20, 2014** – US-CERT notified OPM of malicious activity and OPM initiates investigation and monitoring of adversary.
- **March 2014 to May 2014 –** OPM (under US-CERT guidance) investigated 2014 incident and monitored attackers.
- **April 25, 2014** – The domain "Opmsecurity.org" is registered to Steve Rogers (a.k.a. Captain America).[359] This domain was later used to exfiltrate data from OPM's network.
- **May 7, 2014** – The attacker poses as a background investigations contractor employee (KeyPoint), used an OPM credential, remotely accessed OPM's network and installed PlugX malware to create a backdoor. The agency's forensic logs show "infected machines" were accessed through a VPN connection, which was how background

[356] McClure Tr. at 18.
[357] June 9, 2015 DMAR at HOGR0724-001154.
[358] *Hearing on OPM Data Breach: Part II* (statement of Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt.).
[359] Saulsbury Tr., Ex. 4.

investigation contractors accessed OPM's network. At the time, OPM gave contractors a username and password and investigators would log in with this OPM credential.[360]

- **May 27, 2014** – OPM initiates "Big Bang" to eliminate attackers and complete remediation. This decision was made after OPM observed the attackers "load a key logger onto . . . several database administrators' workstations" and they got "too close to getting access to the PIPs system."[361] Meanwhile, the attacker that established a foothold on May 7, 2014 remained in the OPM network.

- **June 5, 2014 –** Malware is installed.[362] This malware installation appears to have been facilitated through the backdoor established on May 7, 2014.[363]

- **June 2014** – OPM contractor USIS self-detects a cyber-attack on its IT system and notified OPM.[364] USIS investigates and blocks and contains the attacker by early July, and invites US-CERT to USIS facilities to investigate by late July 2014.[365]

- **June 20, 2014** – Attackers conduct a remote desktop protocol (RDP) session indicating the attackers had escalated their access and began moving deeper into the network, contacting "important and sensitive servers supporting . . . background investigation processes." This RDP session was not discovered until 2015.[366]

- **June 23, 2014** – First known adversary access to OPM's mainframe, according to US-CERT.[367]

- **July to August 2014** – Attackers successfully exfiltrate OPM background investigation data. OPM contractor Brendan Saulsbury testified that forensic logs showed "they are sort of touching or accessing the data during the summer of 2014."[368]

---

[360] Wagner Tr. at 127-128; Saulsbury Tr. at 70-71; OPM Cybersecurity Events Timeline; Briefing by US-CERT to H. Comm. on Oversight & Gov't Reform Staff (Feb. 19, 2016). KeyPoint CEO testified that "there was an individual who had an OPM account that happened to be a KeyPoint employee and [] the credentials of that individual were compromised to gain access to OPM." *Hearing on OPM Data Breach: Part II* (statement of Eric Hess, KeyPoint CEO). The OPM Director of IT Security Operations [Wagner] said multiple credentials were compromised during the 2015 incident, but a KeyPoint credential was likely used for the initial attack vector. [Wagner] added "the adversary, utilizing a hosting server in California, created their own FIS investigator laptop virtually. They built a virtual machine on the hosting server that mimicked and looked like a FIS investigator's laptop…and they utilized a compromise KeyPoint user credential to enter the network through the FIS contractor VPN portal." Wagner Tr. at 86.

[361] Saulsbury Tr. at 25-26, at 25-26.

[362] Letter from KeyPoint Government Solutions to the Hon. Elijah E. Cummings, Ranking Member, H. Comm. on Oversight & Gov't Reform (July 2, 2015).

[363] Briefing by US-CERT to H. Comm. on Oversight & Gov't Reform Staff (Feb. 19, 2016).

[364] *Hearing on OPM Data Breach: Part II* (statement of Robert Giannetta, Chief Info. Officer, U.S. Investigations Serv's, LLC). Despite a contractual obligation to notify contractors immediately of a "new or unanticipated threat or hazard", OPM did not notify their contractors (KeyPoint and USIS) of the March 2014 incident. *Id.*

[365] *Hearing on OPM Data Breach: Part II* (statement of Robert Giannetta, Chief Info. Officer, U.S. Investigations Serv's, LLC).

[366] Coulter Tr., Ex. 18.

[367] OPM Cybersecurity Events Timeline.

- **July 29, 2014** – The domain "Opm-learning.org" is registered to Tony Stark (a.k.a. Iron Man).[369]

- **August 2014** – Following public reports of a data security breach at another contractor, OPM requested access to KeyPoint facilities and KeyPoint agreed.[370]

- **August 16, 2014** – The malware installed on June 5, 2014 appears to cease operational capabilities.[371]

- **October 2014** – Attackers move through the OPM environment to the Department of Interior data center where OPM personnel records are stored.[372]

- **December 2014** – Attackers exfiltrate 4.2 million personnel records.[373]

- **March 3, 2015 -** "wdc-news-post[.]com" is registered by attackers. Attackers would use this domain for C2 and data exfiltration in the final stage of the intrusion.[374]

- **March 9, 2015** – Last beaconing activity to the unknown domain "opmsecurity.org" registered to Captain America, attackers switched their attack infrastructure to "wdc-"news-post.com" as their primary C2 domain for the remainder of the intrusion. [375]

- **April to June 2015** – Primary incident response and investigation period.

The timeline outlined above sets the stage for the incident response and forensic investigation that took place in the spring of 2015.

In April 2015, OPM Realized They Were Under Attack – Again

On April 15, 2015, OPM sent an email to US-CERT reporting the presence of four malicious binaries, and what would later turn out to be the first indicators that OPM's systems had been compromised in the largest data breach in the history of the federal government.[376]

---

[368] Saulsbury Tr. at 70. Wagner, the OPM Director of IT Security Operations admitted OPM did not have a "fully logged" environment in the summer of 2014, but they were working toward that end during the summer and through the fall of 2014. Wagner Tr. at 78.
[369] Saulsbury Tr., Ex. 4.
[370] *Hearing on OPM Data Breach: Part II* (statement of Eric Hess, Chief Exec. Officer, KeyPoint Gov't Solutions).
[371] Letter from KeyPoint Government Solutions to the Hon. Elijah E. Cummings, Ranking Member, H. Comm. on Oversight & Gov't Reform (July 2, 2015) (citing US-CERT Report (Aug. 30, 2015).
[372] OPM Cybersecurity Events Timeline.
[373] *Id.*
[374] DOMAIN > WDC-NEWS-POST.COM, THREATCROWD.ORG (last visited June 28, 2016), https://www.threatcrowd.org/domain.php?domain=wdc-news-post.com..
[375] Saulsbury Tr. at 59; *see also* DOMAIN > WDC-NEWS-POST.COM, THREATCROWD.ORG, available at: https://www.threatcrowd.org/domain.php?domain=wdc-news-post.com.
[376] U.S. Dep't of Homeland Security/US-CERT, Preliminary Digital Media Analysis-465355 (May 4, 2015) (OPM Production: Oct. 28, 2016); Briefing by U.S. Office of Pers. Mgmt. to H. Comm. on Oversight & Gov't Reform Staff (Apr. 18, 2016).

Documents and testimony show the initial discovery of the indicators of compromise (IOCs) involved a number of parties, including US-CERT, the FBI, OPM contractors, the OPM IG, and several private companies.

Captain America: The First Indicator that Led to the 2015 Discovery of the Background Investigation Data Breach

In April 2015, OPM discovered and began investigating the first indicator that its systems had been compromised.[377] Director of IT Security Operations Jeff Wagner testified that the first indicator of compromise was an unknown SSL certificate,[378] and was discovered during the rollout of a new version of the security application "Websense."[379] A Secure Socket Layer (SSL) certificate is used to establish a secure channel between an individual's browser and a website. In this case, an OPM computer had been communicating with an unknown website, or domain: "opmsecurity.org."

The Committee obtained documents that show the unknown domain opmsecurity.org was initially brought to the attention of OPM by a contractor, Assurance Data, during the roll out of a new functionality for OPM's Websense technology.[380] Assurance Data identified opmsecurity.org in an email with the subject "RE: OPM Daily Health" on April 14, 2015.[381] OPM was adding groups of users to Websense, as they were transitioning towards filtering all outbound traffic through Websense.[382] During the course of this rollout, Assurance Data observed "a certificate error for the domain called opmsecurity.org."[383]

The next day, April 15, OPM responded to Data Assurance. In an email, an OPM employee described the domain opmsecurity.org as "sketchy at best."[384] The agency "looked up the domain details and observed that it was what appeared to be a spoof domain,"[385] or a domain that was purposely named to emulate legitimate looking websites belonging to or affiliated with OPM. There were clues that "opmsecurity.org" was a spoof domain: "it was a randomized email address,"[386] and it was registered to Steve Rogers, a.k.a. Captain America.

OPM provided to the Committee a document entitled "AAR Timeline" that provided more information about their findings on April 15 and 16 related to the unknown SSL certificate.

---

[377] June 9, 2015 DMAR at HOGR0724-001154; *see also* Saulsbury Tr. at 57-58.
[378] Wagner Tr. at 80.
[379] Saulsbury Tr. at 58.
[380] *Id.*
[381] Email from [redacted] Chief Sec. & Strategy Officer, Assurance Data, Inc. to [redacted] et. al., U.S. Office of Pers. Mgmt. (Apr. 14, 2015, 12:36 p.m..) at HOGR020316- 1887 (OPM Production: Apr. 29, 2016).
[382] Saulsbury Tr. at 58.
[383] *Id.*
[384] Email from [redacted] U.S. Office of Pers. Mgmt. to [redacted] Chief Sec. & Strategy Officer, Assurance Data, Inc., and [redacted] et al, U.S. Office of Pers. Mgmt. (Apr. 15, 2015, 9:50 a.m.) at HOGR020316- 1886 (OPM Production: Apr. 29, 2016).
[385] Saulsbury Tr. at 59.
[386] ThreatConnect Research Team, *OPM Breach Analysis*, THREATCONNECT (June 5, 2015), available at: https://www.threatconnect.com/opm-breach-analysis/..

According to this document, the unknown SSL certificate "[W]as identified and attached to domain "opmsecurity.org" and "six machines [were] identified as communicating with this domain."[387] The AAR Timeline also reported that the domain "opmsecurirty.org" was registered to "a fake email address" under the name "Steve Rogers."[388] Further, the AAR Timeline, noted that an "alert" related to this unknown SSL certificate was initially discovered on February 24, 2015 and the original beaconing traffic to this domain began in December 2014.[389] The AAR Timeline also indicated OPM had identified three work stations and three servers on the OPM network that communicated with the suspicious domain "opmsecurity.org."[390]

The investigation revealed that these machines had also contacted another potentially malicious domain "opm-learning[.]org" – which was registered to Tony Stark, a.k.a. Iron Man – and "wdc-news-post.com." Two of the three suspicious IP addresses—each registered to a Marvel comic book character—was "a really big red flag" for OPM's security team.[391] After running forensic scans OPM was able to determine the suspicious IP address registered to Tony Stark ("opm-learning[.]org") was in fact communicating with malware that was trying to "fly under the radar as if it was a McAfee antivirus executable."[392] This was noteworthy because OPM did not use McAfee.[393] Beginning in 2005, US-CERT had issued alerts that APT attacks often used malware specifically designed to elude anti-virus software and firewalls and mentioned the use of McAfee and Symantec names in connection with these attacks.[394]

After identifying the false IP addresses and the malware, OPM alerted US-CERT.[395] At 6:53 p.m. on April 15, 2015, OPM's Computer Incident Readiness Team (OPM-CIRT) filed a report, INC478069, identifying four malicious binaries – files that OPM considered to potentially be malware or other malicious code. Three of the four malicious binaries reported to US-CERT on April 15, 2015 were identified as having the "potential for a breach or a compromise passed a malware infection."[396] Wagner, OPM's Director of IT Security Operations, also contacted the FBI's CYWATCH to report that the IP addresses and domains associated with the incident as potential C2 servers—the infrastructure necessary for an adversary to conduct an attack.[397]

The Avengers: Anatomy of the Data Breach Discovered in 2015

The first evidence of the attackers' presence comes on May 7, 2014, when the attackers dropped malware (PlugX) onto an OPM server that was one hop away from a machine with

---

[387] AAR Timeline – Unknown SSL Certificate (April 15, 2015) at HOGR020316- 1922 (OPM Production: Apr. 29, 2016).
[388] *Id.*
[389] *Id.*
[390] Saulsbury Tr. at 59.
[391] Saulsbury Tr. at 60.
[392] *Id.*
[393] *Id.*
[394] US-CERT, *Technical Cyber Security Alert TA05-189A: Targeted Trojan Email Attacks* (July 2005)
[395] Saulsbury Tr. at 60.
[396] Coulter Tr. at 14-15.
[397] Email from REDACTED, Fed. Buerau of Investigation Cyber Div to Jeff Wagner, Dir. Info. Tech. Security Operations, U.S. Office of Pers. Mgmt. (Apr. 16, 2015, 2:19 a.m.) at HOGR020316- 1910 (OPM Production: Apr. 29, 2016); *see also* AAR Timeline – Unknown SSL Certificate (April 15, 2015) at HOGR020316- 1922 (OPM Production: Apr. 29, 2016).

direct access to the background investigations and finger print database.[398] Ultimately, these attackers were able to access OPM's Local Area Network (LAN)—the foundational component of OPM's internet infrastructure—and drop PlugX malware.[399]

The PlugX malware, which is a sophisticated piece of malware, allowed the attackers to maintain a presence on OPM's system and network as of May 7, 2015, and it also provided the attackers with other functionality. This malware has an estimated 19,000 lines of code and comes with 13 default, modular plugins.[400] It provides an attacker with a "range of functionality" including the ability to log keystrokes; modify and copy files; capture screenshots or video of user activity; and perform administrative tasks such as terminating processes, logging off users, and rebooting victim machines.[401] PlugX has the ability to give attackers "complete control over the [infected] system."[402]

The PlugX malware, which was the primary piece of malware used in the 2015 data breach, was engineered to covertly beacon back to the "host's network resources [and] establishing a SSL connection to malicious domains (opmsecurity[.]org and wdc-news-post[.]com) and setting the state of a TCP connection."[403] In effect, an SSL connection establishes a secure, or encrypted, link between a server and a website – which in this case was established between the PlugX malware and the malicious domains ("opmsecurity.org" and "wdc-new-post.com").

US-CERT also found these attackers used "opmsecurity.org", primarily associated with the IP address [redacted], as part of their attack infrastructure—the internet components necessary for the attackers to communicate with their PlugX malware throughout the life-cycle of the intrusion.[404] Further, US-CERT found (based on domain firewall logs) that the compromised machines on OPM's network connected with "known malicious IP [redacted]" on January 12 and January 20, 2015.[405]

Other variations of PlugX were found to have been active within the OPM environment throughout the 2014/2015 intrusion. The attacker placed additional, modified versions of PlugX—dubbed by investigators as the "first" and "second" variations—on victim machines on October 10, 2014 and January 31, 2015, respectively.[406] These versions of PlugX were installed months after the key objectives of the intrusion were already achieved. This shows the attacker was continuously modifying and customizing PlugX in order to better customize the malware to OPM's network environment, maintain access, and conceal malicious activities.

---

[398] June 9, 2015 DMAR at HOGR0724-001154.
[399] OPM Cybersecurity Events Timeline.
[400] Roman Vasilenko & Kyle Creyts, *An Analysis of PlugX Malware*, LASTLINE LABS (Dec. 17, 2013), http://labs.lastline.com/an-analysis-of-plugx.
[401] Ryan Angelo Certeza, Pulling the Plug on PlugX, TRENDMICRO (Oct. 4, 2012), http://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/112/pulling-the-plug-on-plugx.
[402] *Id.*
[403] June 9, 2015 DMAR at HOGR0724–001154.
[404] June 9, 2015 DMAR at HOGR0724-001167.
[405] *Id.*
[406] June 9, 2015 DMAR at HOGR0724–001154.

On a related matter, the security research firm ThreatConnect published a February 2015 analysis of the Anthem breach announced on February 4, 2015 that mentioned the "opm-learning.org" domain.[407] Anthem is a health insurance company that held data on as many as 80 million Americans—current and former members of Anthem health plans, and some nonmembers.[408] ThreatConnect attributed the Anthem hack to a threat actor group, variously described as "Deep Panda."[409] In February 2015 (over one month before OPM's April 2015 discovery), ThreatConnect found that this group may have also registered the domain opm-learning.org as part of an intrusion campaign, and noted "OPM had been compromised by a likely state-sponsored Chinese actor in mid-March of [2014]."[410] ThreatConnect warned that because the domain was registered after the breach occurred on July 29, 2014, "OPM could be an ongoing direct target of Chinese state-sponsored cyber espionage activity."[411]

In March 2015, it appears that the attackers changed their attack infrastructure. The attackers switched their command and control servers, installing a new, updated version of malware on infected systems.[412] Consequently, on March 7, 2015, the attackers registered the domain wdc-news-post.com, resolving to the IP address [redacted][413] The domain would switch IP's to [redacted] on May 11, 2015, after the intrusion was already discovered.[414] The switch from opmsecurity.org ([redacted]) to wdc-news-post.com ([redacted]) was accompanied by a new version of PlugX malware, dubbed the "third version" by US-CERT, which would be programed to call-back to the newly-created "wdc-news-post.com" domain.[415]

The March 2015 change in the attack infrastructure could have been prompted by a number of factors. First, it is not uncommon for attackers to use different infrastructure during different stages of the intrusion life-cycle. It is possible large-scale data exfiltration had been completed by spring 2015 and the attackers were moving to a new infrastructure wholly unconnected from that used to effect the initial entry into OPM's network. In the event this intrusion and theft of data was discovered, the infrastructure used would be compromised.

Second, changing the infrastructure would allow the attackers to maintain access to the network should their previous infrastructure be discovered. It is possible open-source threat researchers were dangerously close to independently discovering infrastructure used in the OPM intrusion.

---

[407] Threatconnect Research Team, *The Anthem Hack: All Roads Lead to China*, THREATCONNECT (Feb. 27, 2015), https://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/.
[408] Michael Hiltzik, *Anthem is Warning Consumers About its Huge Data Breach. Here's a Translation*, L.A. TIMES, Mar. 6, 2015, http://www.latimes.com/business/la-fi-mh-anthem-is-warning-consumers-20150306-column.html.
[409] Threatconnect Research Team, *The Anthem Hack: All Roads Lead to China*, THREATCONNECT (Feb. 27, 2015), https://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/
[410] *Id.*
[411] *Id.*
[412] June 9, 2015 DMAR at HOGR0724-001157.
[413] DOMAIN > WDC-NEWS-POST.COM, THREATCROWD.ORG (last visited June 28, 2016), https://www.threatcrowd.org/domain.php?domain=wdc-news-post.com.
[414] June 9, 2015 DMAR at HOGR0724-001157.
[415] *Id.*

The version of PlugX used in the 2014/2015 intrusion had a suite of capabilities that were likley customized for the OPM environment. In describing the malware, US-CERT delineated the capabilities of the particular version of PlugX used in the 2014/2015 intrusion:[416]

> [T]his version of PlugX also is capable of remote access control, file/directory/drive enumeration, file/directory creation, process creation, enumerating the host's network resources, establishing a SSL connection to malicious domains (opmsecurity[.]org and wdc-news-post[.]com) and setting the state of a TCP connection.[417]

The ability to establish an "SSL connection to malicious domains" would become a critical component in the hacker's ability to execute command and control, maintain access, and exfiltrate data out of OPM's network. Hackers used the PlugX to create fake SSL certificates that would allow host machines to connect to the malicious domains "opmsecurity.org", "opm-learning.org", and "wdc-news-post.com."[418] The use of these SSL certificates eventually led to the discovery of the intrusion. In April 2015, OPM security personnel began installing Websense, which gave OPM an enhanced ability to filter SSL certificates.[419] During the Websense roll-out, the newly installed system was able to flag fake SSL certificates to "opmsecurity.org" and other malicious domains.

It is not entirely known how, or even when, the attackers gained access to an OPM network credential held by OPM's contractor KeyPoint, but the attackers were able to use that credential to gain initial access into OPM's network, using a virtual private network (VPN) login to access an OPM SQL server. The attackers also setup remote desktop protocol (RDP) sessions from the SQL server to move laterally, infected additional systems and gained additional footholds until finally connecting to their primary target, the background investigation and fingerprint databases.

The KeyPoint credential was "utilized for the initial vector of infection,"[420] but a number of compromised credentials were used over the course of the data breach.[421] The credential that was used at the initial vector of infection, the point at which the adversary dropped malware to obtain persistent presence, was being used by a KeyPoint employee's account.[422] But that KeyPoint employee did not have administrator credentials, which are necessary to conduct higher-order functions on IT environment. Jeff Wagner testified:

> So the adversary utilized tactics in order to gain domain administrator credentials. Exactly **how they obtained the credentials, we don't have forensic evidence for, but they needed to gain another set of credentials to do operations**. It's not the only set of credentials they utilized to perform operations. So there are multiple stages where various

[416] June 9, 2015 DMAR at HOGR0724 – 001154.
[417] June 9, 2015 DMAR at HOGR0724 – 001154.
[418] Saulsbury Tr. at 58-59.
[419] Saulsbury Tr. at 58-59.
[420] Wagner Tr. at 86.
[421] Wagner Tr. at 86.
[422] Wagner Tr. at 86.

> credentials were used, and though us enforcing PIV killed the capability of them utilizing the KeyPoint credential, they still had persistence from the malware. So they were able to get into the environment through another method to maintain persistence and then utilize domain.[423]

After gaining access to the SQL server, the attacker opened a RDP and dropped malware to maintain a presence on the SQL server. The SQL server itself is significant for its use as the "back end storage" for various OPM applications, including a Jumpbox server used by the administrators that had access to background investigation data. Saulsbury testified "this jumpbox had access into the environments, into the network segments that contained the background investigation systems."[424] The attackers used an RDP to enter the jumpbox and use it "as a pivot point to access all of the systems that were firewalled off from [the] normal network."[425]

The move from the SQL server to the jumpbox was a "lateral movement" by the hackers, and it demonstrates their ability to maintain a presence on OPM's systems, and also to gain the necessary administrator credentials necessary to move from system to system, from computer to computer. Using the jumpbox as a "pivot point," the attackers were able to access the PIPS mainframe, which stored the background investigation data, and "all the FTS boxes" which "are related to the fingerprint transmission system," and finally the human resources department's systems with personnel records stored on systems hosted by the Department of the Interior.[426]

These lateral movements, as evidenced by RDP sessions and the timestamps on the PlugX variants, continued from May into June of 2014.[427] With access to OPM's mainframe as early as June 23, 2014 (and less than one month after the May 27, 2014 "Big Bang"), the attacker would have had access to mainframe applications such as the background investigation data stored on the PIPS system.[428] By early July 2014, the attackers began to exfiltrate the background investigation data. Evidence of data exfiltration would appear to OPM and US-CERT in the form of encrypted RAR archives—"stashes" of stolen data.[429] The attackers continued to exfiltrate the background investigation data through August of 2014,[430] but the fingerprint transaction system data was not taken until March 26, 2015.[431]

---

[423] Wagner Tr. at 86.
[424] Saulsbury Tr. at 75
[425] *Id.*
[426] Saulsbury Tr. at 76-77.
[427] Coulter Tr., Ex. 18.
[428] OPM Cybersecurity Events Timeline.
[429] Coulter Tr. at 25-26. Mr. Coulter would go on to describe the attackers' use of RAR files to exfiltrate data saying, "so as is common in a lot of APT cases, or actually a lot of breaches, if their end goal is to collect data, then they're going to search for it and bring it back to a central point for aggregation. A lot of times data, like this email, if you were to compress it, it would be, you know, potentially one-100th of the size. So RAR, which is a compression format, is used to shrink data. You can also then apply a password to it. So in a lot of cases, where there is data exfiltration or a confirmed breach, it's very common to find these compressed, encrypted stashes of whatever bad guys were after." *See also* June 9, 2015 DMAR at HOGR0724-001156.
[430] OPM Cybersecurity Events Timeline.
[431] June 9, 2015 DMAR at HOGR0724-001158.

The time period from early July 2014, when the attackers begin to exfiltrate the background investigation data, to April 24, 2015, when OPM "successfully eliminates [the] adversary from their systems" represents the data breach end-stage.[432] In this final phase, where the attacker achieves their primary objective – whether it is accessing and exfiltrating data or some other malicious activity – it is important to note this end-stage would have been preceded by an initial penetration through OPM's defenses, an intelligence gathering phase to learn about OPM's network, systems, and security measures. Then after all of this activity the attacker would finally drop the malware and set up the domains necessary to collect and extract data.

The details of the initial phases of the attack and how the 2015 attackers penetrated OPM's defenses and gained sufficient knowledge of OPM's systems so as to quickly begin exfiltrating data, likely will never be known. What is known is how OPM discovered the data breaches announced in June and July of 2015 and how OPM, their interagency partners, government contractors, and private sector incident responders took OPM from the initial indicators of compromise discovered on April 15, 2015 to remediation of the incident in June 2015. Between the first sign of the attackers' foothold on May 7, 2014,[433] to the first exfiltration of data in early July 2014,[434] OPM would complete the "Big Bang"[435] to expel from their network the attackers discovered in 2014. From OPM's perspective by the end of May 2014, the 2014 incident was over – little did OPM know that the 2015 data breach operation was underway.

The following chapter provides additional details on OPM's 2015 discovery and incident response efforts that ultimately led to the discovery of background investigation and personnel records that were exfiltrated – from the perspective of an OPM contractor called Cylance, which was brought in to assist OPM in April 2015.

[432] OPM Cybersecurity Events Timeline.
[433] OPM Cybersecurity Events Timeline.
[434] OPM Cybersecurity Events Timeline.
[435] Email from Press Secretary, U.S. Office of Pers. Mgmt., to Jeff Wagner, Dir. of IT Sec. Operations, U.S. Office of Pers. Mgmt. (June 18, 2015, 8:01 p.m.) at HOGR 020316-000266-67 (OPM Production: Feb. 16, 2016).

Chapter 4: The Role of Cylance Inc.

Cylance Inc.'s information security tools detected critical malicious code and other threats to OPM's network in April 2015. While Cylance tools were available to OPM as early as June 2014, OPM did not deploy its preventative technology until after the agency was severely compromised and the nation's most sensitive information was lost. OPM's IT security operations recommended deploying Cylance's preventative technology, CylanceProtect (Protect), to insulate OPM's enterprise from additional attacks after it became aware in March 2014 of a data breach whereby sophisticated adversaries targeted background investigation data.[436] The Committee obtained documents and testimony that show internal bureaucracy and agency politics trumped security decisions, and that swifter action by OPM to harden the defenses of its enterprise architecture by deploying Protect would have prevented or mitigated the damage that OPM's systems incurred.

OPM's "Cyber Climate" During Cylance Product Demonstrations

In June 2014, OPM began evaluating numerous products, including two Cylance products, for possible use in its legacy environment.[437] The agency's consideration of these tools occurred at a time when the agency was aware its existing environment had been compromised and vulnerabilities had been exploited by a sophisticated adversary.

On March 20, 2014, US-CERT notified OPM that data had been exfiltrated from OPM's system.[438] Agency officials later testified this data breach resulted in the loss of security documents and manuals about high-valued systems and applications on its enterprise architecture, but downplayed the significance of these documents.[439] US-CERT's June 2014 OPM Incident Report highlighted the sophistication of the attackers, which used "an extremely stealthy form of malware [a Hikit rootkit] designed to hide its malicious processes and programs from the detection of commodity intrusion detection and anti-virus products."[440] A rootkit is malicious piece of software that uses administrator or "root" access to modify system settings to hide malware and malicious code at lower layers of an operating system, rendering itself and adversary activity almost undetectable by common anti-malware software.[441]

From March 20, 2014 to May 27, 2014, OPM and US-CERT observed the attackers to learn more about their tactics, techniques, procedures (TTP's), and objectives – including the exfiltration of data.[442] In the final US-CERT June 2014 OPM Incident Report, US-CERT stated:

---

[436] Wagner Tr. at -92.
[437] McClure Tr. at 14.
[438] June 2014 OPM Incident Report at HOGR0818-001233.
[439] *Hearing on OPM Data Breach: Part II* (exchange between Chairman Jason Chaffetz and OPM Dir. Katherine Archuleta and OPM Chief Info. Off. Donna Seymour).
[440] June 2014 OPM Incident Report at HOGR081-001234; *see supra* Chapter 2 The First Alarm Bell – Attackers Discovered in 2014 Target Background Information Data and Exfiltrate System-related data
[441] *What is a Rootkit*, AVG available at: https://support.avg.com/SupportArticleView?l=en_US&urlName=What-is-rootkit.
[442] June 2014 OPM Incident Report at HOGR0818-001233.

> [T]he attackers primarily focused on utilizing [Server Message Block] commands to **map network file shares of OPM users who had administrator access or were knowledgeable of OPM's [Personnel Investigations Processing System] system**. The attackers would create a '**shopping list**' of the available documents contained on the network file shares. After reviewing the 'shopping list' of available documents, the attackers would return to copy, compress, and **exfiltrate the documents** of interest from a compromised OPM system to a [Command and Control] server.[443]

The discovery of a successful intrusion and data breach in the spring of 2014 put OPM on notice. Sophisticated attackers defeated their information security measures and practices, and remained unnoticed as far back as July 2012.[444] The attackers had a clear objective: the background investigation material contained in PIPS. In other words, OPM had every incentive to take swift, decisive action to immediately fortify its legacy systems against a persistent threat that already had secured an advanced understanding of OPM's environment, including its highest valued targets.

The agency purchased select tools from various vendors in June 2014,[445] but declined at this juncture to purchase a key preventative tool recommended by the OPM Director of IT Security Operations called CylanceProtect[446] and only bought its more limited tool, CylanceV.[447] The agency's security personnel remained interested in Protect, and Cylance arranged an extended demonstration in early 2015.[448] When OPM identified an indicator of compromise on April 15, 2015, the agency turned to Cylance for assistance.[449] As soon as OPM began using the Cylance tools in April 2015, it immediately began finding the most critical samples of malicious code on its network.[450] Cylance tools identified a significant amount of malware on OPM's network within 48 hours,[451] and Cylance personnel quickly recognized the agency's cyber situation was dire.[452] Cylance personnel even confided to each other internally over e-mail: "They are fucked btw."[453]

By April 2015, it was too late to undo the damage. Following the May 27, 2014 Big Bang, OPM decided not to purchase and deploy Protect as a result of internal bureaucratic

---

[443] June 2014 OPM Incident Report at HOGR081-001234-35.
[444] June 2014 OPM Incident Report at HOGR081-001235.
[445] OPM Tactical Toolset Purchase, Kick-off and Completion Timeframes (Oct. 21, 2015) (Imperatis Supplemental Document Production: Oct. 21, 2015) (on file with the Committee).
[446] Wagner Tr. at 91-92; *see also* McClure Tr. at 85-86.
[447] McClure Tr. at 19-20.
[448] *Id.*
[449] Coulter Tr., Ex. 2; E-mail from Matthew Morrison, Assurance Data, Inc., to Jeff Wagner, Dir. Info. Tech. Security Operations, U.S. Office of Pers. Mgmt. (Apr. 15, 2015, 10:48 p.m.) at HOGR020316-001899. (OPM Production: Apr. 29, 2016).
[450] Coulter Tr., Ex. 3; Saulsbury Tr. at 72; Email from [redacted] to Brendan Saulsbury, Senior Cyber Sec. Engineer, SRA (Apr. 17, 2015, 5:19 p.m.) at HOGR0724-000872- 75 (OPM Production: Dec. 22, 2015).
[451] Coulter Tr., Ex. 3; Saulsbury Tr. at 72.
[452] McClure Tr., Ex. 9; Coulter Tr., Ex. 5.
[453] *Id.*

hurdles and "political challenges on the desktop."[454] The Big Bang remediation proved unsuccessful; the malicious actor linked to the theft of personnel records, background investigation data, and fingerprint exfiltration had already gained a foothold in OPM's system by May 7, 2014.[455] The malicious actor downloaded PlugX malware on May 7, 2014 on a key Microsoft SQL server[456] at OPM, and had moved laterally across the network to access the PIPS mainframe (which holds background investigation data) on or about June 23, 2014.[457] The attackers ultimately exfiltrated background investigation data from early July through August 2014, and then exfiltrated personnel records in December 2014 and fingerprint data in March 2015.[458]

Overview of the Cylance Cyber Tools

In June 2014, Cylance and OPM personnel began conversations about the potential use of Cylance's products in the agency's legacy (existing) information technology environment.[459] At this time, Cylance offered two products to the marketplace.

CylanceV (V) is a detection product used on end-point devices (i.e., desktop computers, laptops, etc.). First available to the marketplace in October 2013, V software scans endpoints to determine "whether or not something is malicious on a computer."[460] Deployment of V is limited to one endpoint at a time. The product is focused on detection—rather than prevention—of a cyber threat. Cylance CEO Stuart McClure testified that V "will find where an infection might already be or exist, and that will help IT operations to go into the computer, clean it up, fix it up, and do whatever they want to that system. But V is not preventive. It just is after the fact [it] will catch something."[461]

Protect, on the other hand, is designed to prevent malicious activity. It is distributed throughout an enterprise where it utilizes mathematics and algorithms to determine "good" from "bad." That is, it seeks to identify and address items that do not belong within an enterprise that could be a threat. The agency's threat detection and initial response efforts in the wake of the March discovery revolve, in part, around the two modes available through Protect: "Alert" and "Auto Quarantine."

In Alert mode, Protect places the onus on the administrator running the tool to determine whether or not Protect has identified a malicious computer process that should be quarantined, or if it should be "white listed" and remain operating on the environment. When

---

[454] McClure Tr., Ex. 4; McClure Tr. at 44-45.
[455] OPM Cybersecurity Events Timeline.
[456] June 2014 OPM Incident Report at HOGR0724-001154; OPM Cybersecurity Events Timeline.
[457] Coulter Tr. at 79-82, Ex. 18 (Email from Christopher Coulter to Jonathon Tonda); OPM Cybersecurity Events Timeline.
[458] OPM Cybersecurity Events Timeline; Briefing by US-CERT to H. Comm. on Oversight & Gov't Reform Staff (Feb. 19, 2016); June 9, 2015 DMAR at HOGR0724-001158.
[459] McClure Tr. at 14 (The Cylance sales team was introduced to IT security personnel at OPM through Assurance Data. Cylance's sales staff, Nicholas Warner, was introduced to IT security personnel through Mathew Morrison at Assurance Data); McClure Tr. at 12-13 (Assurance Data maintained a re-seller arrangement with Cylance).
[460] McClure Tr., Ex. 1; McClure Tr. at 8.
[461] McClure Tr. at 8.

Protect is operating in "Auto Quarantine" mode, it automatically removes and quarantines threats, thereby requiring no intermediary action. McClure testified: "[Protect] sits on a computer in real time and watches everything that happens on a computer. And every single element of the computer determines whether it's good or bad, whether it's safe or unsafe, malicious or not. And if it's malicious, it stops it. It blocks it. It doesn't even allow it to start. So true -- true prevention."[462]

According to McClure, V:

> [R]equires a user to actually hit a button that says point to this drive or point to this computer or this share, whatever, now hit scan. It requires a physical body to do something like that. Whereas, CylanceProtect, the agent, can be completely hands-free. . . . If you just set it into auto quarantine mode, just forget it. If you have an alert mode, of course, then you have to review the alerts hopefully and then try and quarantine whatever things you find that are bad in there.[463]

April 15-16, 2015: The First 24 Hours

On April 15, 2015, OPM reported to US-CERT the first indicator of compromise.[464] This led to OPM's June and July 2015 announcements regarding the loss of 4.2 million personnel records, 21.5 million background investigation, and 5.6 million fingerprints. At this time, OPM owned V, but had not yet purchased Protect.[465]

OPM Director of IT Security Operations Jeff Wagner described how malware was discovered in 2015. Wagner testified that an indicator was found, then it was followed back to an infected server, and then the search began for the malware on the infected server.[466] Wagner testified:

> [T]he initial malware discovery on an infected machine is normally not done by, say, a tool. It's done once you find an indicator and that indicator points back. Then you use a tool such as Mandiant or Carbon Black or Cylance or various tools to do an overall search, because once you find one piece and you get additional indications, you can then look for other indications as well.[467]

Wagner testified that the unknown SSL certificate was "discovered by Websense" and that "Cylance would have found the specific malware on the machine. And then one of the engineers would have reverse engineered the malware to find it written within the malware."[468]

---

[462] McClure Tr. at 8-9.
[463] McClure Tr. at 46-47.
[464] June 9, 2015 DMAR at HOGR0724-001154.
[465] McClure Tr. at 20.
[466] Wagner Tr. at 54.
[467] Wagner Tr. at 54-55.
[468] Wagner Tr. at 80.

On June 17, 2014, the agency purchased an upgraded version of Websense[469] to replace an older Websense to "enhance the capability to include protection of remote users while attached to foreign networks."[470] Documents show the upgrade started on September 9, 2014 and was completed by September 17, 2015.[471]

By April 2015, OPM's IT Security Operations began to deploy the upgraded version of Websense and during this deployment process identified an initial indicator of compromise.[472] Saulsbury testified:

> We originally detected [a problem] during the course of the Websense rollout as we were sending groups of users, adding more and more groups of users to the pilot group, to have all of their outbound traffic being filtered through Websense. One of the things that we were doing was SSL decryption. Because that is such an intrusive method of inspection, we were monitoring for errors with SSL certificates that were potentially breaking access to applications, updates, and things like that.[473]

Saulsbury continued to describe the findings while rolling out Websense saying:

> [W]e also looked at the IP [sic] domain resolved to and put it into NetWitness. We were able to see that going back we had these three machines that were going through Websense, but we also had three servers that had been contacting this IP address. It looked very strange because there wasn't any business connection between these users' work stations and these three different servers. So that is when the red flag started to go up as this could potentially be malicious activity.[474]

At 6:53 p.m. on April 15, 2015, OPM's Computer Incident Readiness Team (OPM-CIRT) filed a report, INC478069, with US-CERT, and it was assigned incident number INC000000459698.[475]

---

[469] *Raytheon|Websense is Now Forcepoint*, FORCEPOINT, available at: https://www.forcepoint.com/raytheonwebsense-now-forcepoint, ("On January 14, 2016, Raytheon | Websense® announced that it was rebranding the product Forcepoint™ as part of a new venture between Raytheon and Vista Equity Partners").

[470] List of Tactical Security Products (Imperatis Production: Oct. 21, 2015).

[471] *Id.*

[472] Saulsbury Tr. at 58.

[473] *Id.*

[474] Saulsbury Tr. at 59.

[475] E-mail from [redacted] to CIRT (OPM) (Apr. 15, 2015, 6:54 p.m.) at HOGR0724-000868 (OPM Production: Dec. 22, 2015).

From: [redacted]
Sent: Wednesday, April 15, 2015 6:54 PM
To: CIRT
Subject: Follow-Up on Incident call number: INC000000459698 regarding 06-Investigation INC478069

US-CERT has received your report INC478069 and has assigned incident number INC000000459698, for future reference.

Incident Submit Date: 4/15/2015 6:53:18 PM

Thank you,

US-CERT Operations Center

As OPM began to grapple with the developing cyber incident, the agency also discussed the possibility of using Cylance tools to stop the malware from functioning.[476] The documents show there was already a high degree of familiarity with the Cylance products and their capability, but that OPM did not have full access to the tools.[477]

Message

From: Matthew Morrison [redacted]
Sent: 4/15/2015 10:48:33 PM
To: Wagner, Jeffrey P. [redacted] EXCHANGE ADMINISTRATIVE GROUP [redacted] ECIPIENTS/CN=JPWagner]
Subject: Cylance

I also have Cylance on ready to deploy protect to the windows desktop and servers. It WILL stop malware from running.

matt

Use Only

As of the evening of April 15, 2015, OPM owned V, but did not have the latest version of V nor did OPM have access to Protect, the preventative tool.[478] The next morning (April 16) Cylance offered assistance to OPM as the agency was attempting to point V at endpoints, and soon thereafter provided technical support to OPM via conference call to help OPM overcome "incompatibility" issues.[479]

Chris Coulter, Cylance's Managing Director of Incident Response and Forensics, testified that "[OPM was] trying to use [V] against a forensic image, and the methods to do so aren't

[476] E-mail from Matthew Morrison, Assurance Data, Inc., to Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt. (Apr. 15, 2015, 10:48 p.m.), at HOGR020316-001899. (OPM Production: Apr. 29, 2016).
[477] *Id.*
[478] Coulter Tr., Ex. 2 (In this email, Matthew Morrison (with Assurance Data) wrote to Grant Moerschel (Cylance Sales Engineer), seeking the latest Cylance versions, copying Nicholas Warner (Cylance sales director), OPM personnel and OPM contractors, including Jeffrey Wagner (OPM Director of IT Security Operations)).
[479] Coulter Tr., Ex. 2; McClure Tr. at 65.

clearly documented because it's more of a trade craft to know how to do that."[480] Coulter offered to be onsite at OPM the following morning if the incompatibility issue with V was not resolved.[481] Jonathan Tonda (then an OPM contractor in IT Security Operations) replied: "We were able to resolve the issue and obtain results from Cylance. Thanks for your help!"[482]

Highly Confidential CYLANCE_000689

>>
>>
» From: Tonda, Jonathan D. [mailto:[redacted]
» Sent: Thursday, April 16, 2015 4:19 PM
» To: Chris Coulter;
> [redacted]
> Wagner, Jeffrey P.
» Cc: [redacted]; Saulsbury, Brendan S.
» Subject: RE: Cylance Versions

» Hi Chris,

» We were able to resolve the issue and obtain results from Cylance. Thanks
> for your help!
» --Jon

At 3:56 p.m., Saulsbury sent Wagner a list of four malicious executables identified by V that were residing on OPM servers, and each malicious executable was assigned a score under the Cylance rating system.[483] McClure described this rating system in his testimony to the Committee. He stated:

> So we rank and score files and executional elements in a spectrum from positive 1 to negative 1. Anything from a positive 1 to a zero is considered safe mathematically. Anything from zero to negative .8 is considered abnormal. And then from negative .8 to negative 1 is considered unsafe.[484]

Three of the four malicious executables found by V on April 16, 2015 were rated -1 and the fourth was rated -.93 on the Cylance scale.[485] Coulter testified that the files showed "That there's a potential for a breach or a compromise [past] a malware infection."[486] One of the four files included a Windows Credentials Editor (WCE). Coulter described the significance of the WCE finding:

> So malware, while, as nasty as it can be, is fairly common, at least in a broad sense. Somebody actually has to use that malware for it to be malicious, most of the time. When you see something like a confirmed Windows Credentials Editor of other types of credential dumping tools, **that's usually a sign of an overt act, so something that somebody with ill intent actually was trying to achieve** versus just a presence of a

[480] Coulter Tr. at 10-11.
[481] Coulter Tr., Ex. 2.
[482] *Id.*
[483] Coulter Tr., Ex. 3.
[484] McClure Tr., Ex. 87-88.
[485] Coulter Tr., Ex. 3.
[486] Coulter Tr. at 14-15.

> malicious file, which may or may not have been used. A WCE 64 doesn't just appear for -- just to have it there. It usually is used.[487]

US-CERT would later confirm WCE as a "hack tool."[488]

On April 15, OPM found another suspicious file—a McAfee dynamic link library (DLL) called "macutil.dll" that Saulsbury recalled in testimony as being integral to the attacks:

> So we took Cylance V and put it on the known infected machine with the McAfee macutil.dll malware -- so the machine with the mcutil.dll malware and then we ran Cylance V on it to scan the machine for malicious artifacts. And what it came up with is it successfully identified that mcutil.dll file as malware.[489]

The McAfee file was highly suspicious because OPM did not use McAfee in its systems. Saulsbury stated: "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."[490] The next day, US-CERT confirmed the malicious nature of this file.

April 17, 2015: US-CERT Confirms PlugX

On Friday, April 17, 2015 at 11:39 a.m., Saulsbury processed a new malware submission to US-CERT for its review that included the files he shared with Wagner the night before.[491] At 5:19 p.m., US-CERT reported to OPM its initial analysis of the executable files.[492]

US-CERT reported that the mcUtill.dll was a "loader"—an operating system component that copies programs to memory. When executed by a seemingly innocuous executable (mcsync.exe), mcutill.dll decrypts, decompresses, and loads a third file into memory (mcsync.eal). This file is the primary file – or payload – for a remote access tool (RAT) called PlugX. Each of these files was contained within a "McAfee.SVC" folder, which also contained an output file for the keylogger ([redacted]). PlugX used the malicious domain "wdc-newsport.com" for command and control.[493]

In other words, the four files contained in the folder, which resided within a directory called '[redacted]" worked in concert to harm OPM, and did so in a way that was hard to detect. Each of the four files had a specific function:

---

[487] Coulter Tr. at 16.
[488] U.S. Dep't of Homeland Security/US-CERT, Malware Analysis Report-460357 (April 17, 2015) at HOGR0092 (OPM Production: Dec. 22, 2015).
[489] Saulsbury Tr. at 66.
[490] Saulsbury Tr. at 60; email from [redacted] to Brendan Saulsbury, Contractor OPM IT Security Operations (Apr. 17, 2015, 5:19 p.m.) at HOGR0724-000872- 75 (OPM Production: Dec. 22, 2015).
[491] Email from [redacted] to Brendan Saulsbury, Contractor OPM IT Security Operations (Apr. 17, 2015, 5:19 p.m.) at HOGR0724-000872- 75 (OPM Production: Dec. 22, 2015).
[492] *Id.*
[493] *Id.*; June 9, 2015 DMAR at HOGR0724-001157.

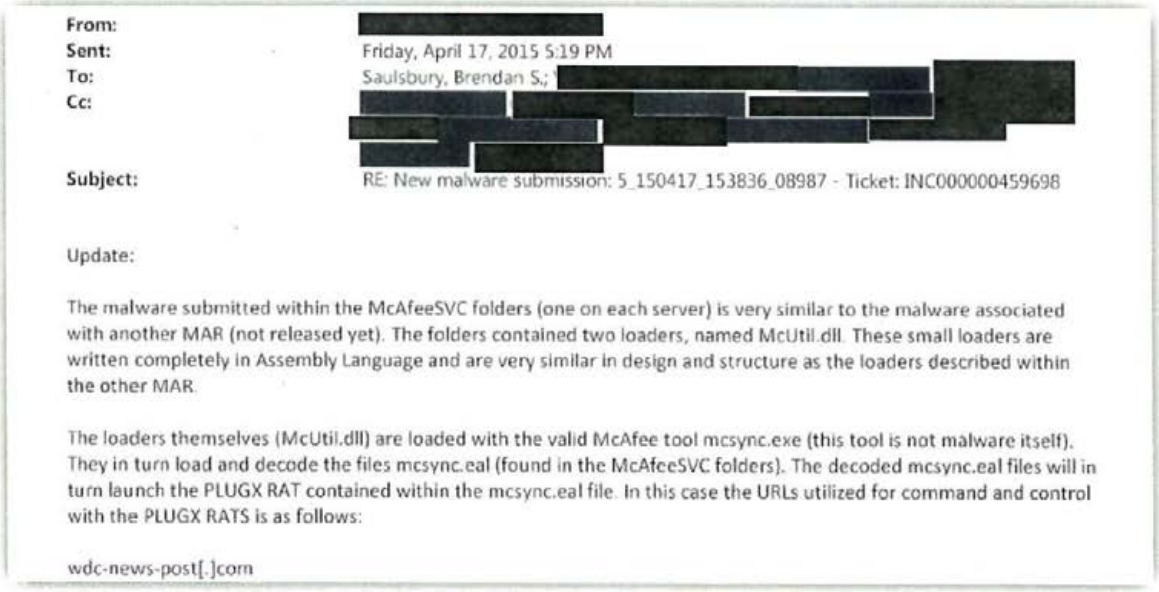
- Mcsync.eal is an encrypted .dll file and PlugX malware considered malicious. After analysis of the Master File Table (MFT), US-CERT found that the file was time-stamped. Documents show the creation date was March 9, 2015 at 6:13:01 a.m.

- Mcsync.exe is a binary itself and is innocuous; however, it is used to load the PlugX malware through McUtil.dll. Analysis of the MFT shows the file was time-stamped. Documents show the creation date was March 9, 2015 at 6:13:01 a.m.

- McUtill.dll is a binary that has been identified as a PlugX loader. It attempts to connect to the malicious domain "wdc-news-post[.]com" which resolves to IP [redacted] US-CERT found the attacker time-stamped the file. Documents show the creation date was March 9, 2015 at 6:13:01 a.m.

- Adb.hlp was found to be the output file created to store the key strokes recorded by mcsync.eal. In addition to key-logging, this version of PlugX is capable of remote access control, file/directory/drive enumeration, file/directory creation, process creation, enumerating the host's network resources, and establishing a SSL connection to malicious domains.[494]

US-CERT reported PlugX was located in two OPM directories: a McAfee folder ("[redacted]") and a directory called ("[redacted]").[495]



From: [redacted]
Sent: Friday, April 17, 2015 5:19 PM
To: Saulsbury, Brendan S.; [redacted]
Cc: [redacted]
Subject: RE: New malware submission: 5_150417_153836_08987 - Ticket: INC000000459698

Update:

The malware submitted within the McAfeeSVC folders (one on each server) is very similar to the malware associated with another MAR (not released yet). The folders contained two loaders, named McUtil.dll. These small loaders are written completely in Assembly Language and are very similar in design and structure as the loaders described within the other MAR.

The loaders themselves (McUtil.dll) are loaded with the valid McAfee tool mcsync.exe (this tool is not malware itself). They in turn load and decode the files mcsync.eal (found in the McAfeeSVC folders). The decoded mcsync.eal files will in turn launch the PLUGX RAT contained within the mcsync.eal file. In this case the URLs utilized for command and control with the PLUGX RATS is as follows:

wdc-news-post[.]com

[494] June 9, 2015 DMAR at HOGR0724-001154. A US-CERT *Digital Media Analysis Report* provides detailed analysis and insight into the specific tactics, techniques, and procedures (TTPs) observed on the media submitted for analysis.
[495] June 9, 2015 DMAR at HOGR0724-001155.

April 17, 2015: CylanceProtect Deployed

On April 17, 2015, Coulter arrived at OPM's headquarters in Washington, D.C., to provide on-the-ground assistance.[496] That day, OPM decided to deploy Protect, but only in "Alert" mode (not in auto-quarantine mode).[497] Since OPM had been familiar with the product since June 2014, but still did not execute a purchase, Cylance staff was skeptical about whether this time the agency was truly moving to purchase and deploy Protect.

Cylance sales engineer Grant Moerschel emailed Coulter: "Is this a [Proof Of Concept] in their mind or the start of a real deployment?"[498] Coulter replied: "Not entirely sure what the back stories are, all I know is they want this on all systems by the end of today."[499] Director of Sales Nick Warner replied: "It's go time!"[500]

To: Nicholas Warner >, [redacted]
Subject: RE: OPM Protect Access
Awesome!!!

of our license, I believe."[501] As of April 17, 2015, OPM had not purchased a Protect license and did not purchase such as license until June 30, 2015.[502]

Nonetheless, Cylance provided OPM full access to Protect in mid-April 2015 on a demonstration basis and without purchasing a license because as Cylance testified it was evident OPM was under attack and they deemed it the appropriate course of action. McClure testified:

> A. Yes. So typically, like we say, an evaluation of this sort would be a small evaluation. However, when it's under these kind of incident response emergency situations, we allow them to install on as many boxes as they want. Because we just want to help them, provide them the support, get them to be able to identify the problems and then prevent them, clean it as quickly as humanely possible, get the bad actors out of the company, organization. So we allowed them to install on all of them, as many systems as they had -- a little unusual for an evaluation but not completely unusual, especially under these circumstances.
>
> Q. Those circumstances being?
>
> A. That **they were under severe attack and had been for quite some time.**
>
> Q. And you just described incident response efforts going on. Are you aware of the sense of urgency in how OPM was responding to what they found and flagged for your attention the day before?
>
> A. Once we were engaged on April 16th, 17th, it was very much a fire drill, every 24 hours. And they were taking it very, very seriously from all of our observations, and reacting as quickly as possible, and getting as much help as they could, and engaging with us, and getting the technology out there, and trying to quarantine as quickly as possible. It's actually one of the poster-child examples of how to do it properly in an investigation, just as soon as you humanely possibly know that you've been breached, to try and roll out this new tech. I think they did an admirable job.[503]

With respect to why OPM utilized Cylance tools in April 2015, Wagner testified:

> We were uncomfortable with just trusting that we knew all the indicators of compromise. And so we obtained the Cylance endpoint client and

---

[501] Wagner Tr. at 95.
[502] McClure Tr., Ex. 1; *see also* Cylance Purchase Order from Assurance Data, Inc. (June 30, 2015), at CYLANCE 000018 (Cylance Production: Dec. 17, 2015).
[503] McClure Tr. at 58-59.

deployed it, and then a Cylance engineer helped make sure we got it configured correctly to get proper information out of it."[504]

Wagner also testified that Cylance was able to find things other tools could not "because of the unique way that Cylance functions and operates. It doesn't utilize a standard signature of heuristics or indicators, like normal signatures in the past have been done, it utilizes a unique proprietary method."[505]

April 18, 2015: Protect Lights Up Like a Christmas Tree

On April 18, 2015, one day after deploying Protect, OPM rapidly escalated its use throughout the enterprise. McClure wrote: "I checked in on the deployment and we are at 2226 devices at last count. Tons of findings. Chris is working through them already quarantining. It is juicy."[506] McClure testified: "[**W]e were finding a ton of malicious attacks** on -- on the boxes that we were getting deployed to."[507]

On April 18, however, OPM was not yet utilizing Protect's full capability. The agency was using the product in "alert" mode and not "auto quarantine" mode.[508] Agency personnel therefore had to determine what should be stopped from operating in OPM's environment after reviewing alerts. When McClure stated in the April 18th email that "Chris is working through them…", this statement describes the steps that must be taken to evaluate each item OPM was alerted to before agency personnel could then consciously address them (i.e., extracted from the environment, white listed, etc.). McClure testified that **only about ten percent of Cylance's customers use the alert-only mode** and in alert-only mode, the product "will alert only when an attack is present or happening in the system."[509]

Wagner testified that OPM was running Protect in "passive mode, because we didn't want the tool to automatically end up deleting forensic evidence that we needed."[510] That is not how Protect works. McClure testified: "[W]hen we quarantine a file, we don't actually delete it yet. The rationale is, if we quarantine something by mistake, that's a false positive. In that rare instance, the customer would want to unquarantine it to put it back in production. So we keep it in a secure, untamperable space on disk that allows us to perform that unquarantining. Unfortunately, that does take up space as part of the quarantine area."[511]

Protect identified 39 "Trojans" on various parts of OPM's network that were rated a negative one (-1) on the Cylance rating scale—the worst possible rating—and Cylance staff recommended quarantining these items.[512] The finding of 39 Trojans was significant because as Coulter testified the "Trojan's" functionality allows the attacker to "bypass to some degree

[504] Wagner Tr. at 87-88.
[505] Wagner Tr. at 96.
[506] McClure Tr., Ex. 8.
[507] McClure Tr. at 25.
[508] McClure Tr., Ex. 8.
[509] McClure Tr. at 10-11.
[510] Wagner Tr. at 94.
[511] McClure Tr. at 71.
[512] Coulter Tr., Ex. 4.

security controls and allow a bad actor, in some cases, unrestricted access to a network."[513] Coulter stated: "Any one Trojan could have that capability."[514]

In fact, when reviewing the work ticket that identified these 39 Trojans, Coulter testified: "**To say it bluntly, [Protect] lit up like a Christmas tree.**"[515] According to Coulter, Cylance's team concluded these were downloader files, which are typically associated with malware and multiple Trojans.[516] When asked these results caused concern, Coulter stated: "**Having gone through security clearance process many times, I know what OPM does. And dealing with APT almost on a daily basis, you put two and two together. You can just assume the risk that, you know, what could unfold or what could be there.**"[517]

April 19, 2015: Severity of the Situation Becomes Clear

It quickly became clear to Cylance that the IT security situation at OPM was dire.[518] By April 19, 2015 malicious items continued to be found in OPM's enterprise.

From: Chris Coulter
Sent: Sunday, April 19, 2015 10:49 AM
To: Stuart McClure
Cc: [redacted]
Subject: OPM

They are fucked btw… Walking their forensic guys through some analysis and I pointed them to an encrypted rar archive of some bad stuff. Stu can we use Brians GPU rig to crack them? Not seeing the common bat/vbs that would give us the password easily.

Chris Coulter
Consulting Director

In an April 19 email, Coulter reported to McClure that he had identified "an encrypted rar archive of some bad stuff." McClure told the Committee a "RAR" file is "a compressed encrypted archive of other files" that he recalled "seeing evidence of an attack that had already been there, been successful, and it was nasty" and that "[t]here were signs of ex-filtration of data, yes."[519] In order to address the "encrypted rar archive" finding, Coulter asked for assistance with another tool to help break the encryption. McClure testified:

> [W]hen forensic folks like us get on-site and take a look at these things, we can't easily open them and see what they've been able to steal and push out of the environment without using something like a GPU [Graphics Processing Unit] password-cracking rig, which is what's

[513] Coulter Tr. at 50.
[514] Coulter Tr. at 80.
[515] Coulter Tr. at 20-21.
[516] Coulter Tr. at 20-21.
[517] Coulter Tr. at 21.
[518] McClure Tr., Ex. 9; Coulter Tr., Ex. 5.
[519] McClure Tr. at 27.

> referenced here. . . So he's saying, you know, I'm not seeing the common BAT or VBS files that would give us the passwords easily. So typically, BAT is short for batch files, and they are Windows batch files. And VBS is short for visual basic scripting or script, both of which help automate certain commands that are run on a computer system. And oftentimes, because hackers are lazy, they'll put into the batch or the VBS scripts, the actual hard-putted password of the encrypted RAR, so that they can help automate both encryption and decryption of it in their tasks.[520]

On April 19, the signs of a significant compromise at OPM were clear. Coulter testified:

> They're in a severe situation. . . . It's an incident now. It's much more than just a malware incident. So when I was talking earlier about, you know, credential dumping tools and overt actions, **this is again another overt action**. If you don't usually -- if you can't explain why you have a large encrypted RAR archive in a location that most administrators would recognize, there's -- it's likely a stash of something.[521]
>
> * * *
>
> So as is common in a lot of APT cases, or actually a lot of breaches, if their end goal is to collect data, then they're going to search for it and bring it back to a central point for aggregation. A lot of times data, like this email, if you were to compress it, it would be, you know, potentially one-100th of the size. So RAR, which is a compression format, is used to shrink data. You can also then apply a password to it. So in a lot of cases, where there is data exfiltration or a confirmed breach, it's very common to find these compressed, encrypted stashes of whatever bad guys were after.[522]

Like McClure, Coulter also testified that, as of April 19, 2015, a significant chance existed that data from OPM had been exfiltrated.[523] US-CERT's analysis validated their concerns. According to US-CERT:

> Analysis of the image revealed that several variants of PlugX once resided on the victim machine, with the last variant from downloaded folder RAR SFX2 still residing. Several password protected RAR files were found on the victim machine which have been identified by the customer as exfiltrated data.[524]

---

[520] McClure Tr. at 27-28.
[521] Coulter Tr. at 25-26.
[522] Coulter Tr. at 26-27.
[523] Coulter Tr. at 27.
[524] June 9, 2015 DMAR at HOGR0724-001156.

RAR Files

A Roshal Archive or RAR file is a means to compress and encrypt data, which facilitates moving large amounts of data more easily and securely. Compression diminishes network footprint and encryption concealed contents of malicious files or stolen data, making it more difficult for security software to detect the malicious actors' activities.

RAR files have three notable qualities that help explain their usage in the 2015 data breach:

(1) Compressed – the overall file size is reduced and simplified, allowing it to take up less space on disk and making it easier to move around OPM's internal systems, and exfiltrated from its network.
(2) Encrypted – the contents of the RAR files are obfuscated, hidden beneath layers of encrypted code; and conceal their contents.
(3) Unpackability – when executed, RAR's "extract" their contents, creating a directory to place the files they compress and encrypt.

The three variants of PlugX malware used in the 2015 data breach can be tied to RARSFX0, RARSFX1, and RARSFX2 respectively, and give forensic investigators clues as to where the attackers were on OPM's systems and when.

The RAR files that had been identified were notable because these files were ultimately linked to the data exfiltration of the background investigation and fingerprint data and personnel records. For example, RAR SFX2 appears to contain FTS data held on the attackers' primary foothold – WDC-new-post.com.[525] Another, RAR SFX2, when downloaded created the "McAfeeSVC" folder in a directory ("[redacted]") located on a key Microsoft SQL server [redacted][526] and its duplicate server [redacted]. This location gave attackers access to a key jump box that facilitated access to other segments of OPM's environment—segments that house sensitive information.[527] US-CERT found the attacker was active on that server stating: "the first appearance by the actor that was observed on the victim images was on 5/7/2014 at 11:12:25PM from a SQL Server."[528]

US-CERT's analysis of this string of malicious activity would later point out the liability to the country: "It is interesting to note the machine had an [remote desktop protocol] session with [United States Governmen[redacted] system [redacted] on 10/22/2014."[529] In other words, US-CERT was pointing out a remote desktop session that occurred in October 2014 on the system that led to a tunnel (Interior Business Center) at the Department of Interior (DOI) and to the federal employee personnel records that were stolen. US-CERT and OPM would later affirm that the attacker pivoted to the data center at DOI in October 2014, with the personnel records subsequently being exfiltrated in December 2014.[530]

In an exchange with Rep. Robin Kelly (IL), DOI's CIO, Sylvia Burns would later testify before the Committee about how the attacker traversed onto DOI's network and stole the personnel records:

> Ms. KELLY. Thank you, Mr. Chairman. Ms. Burns, the two data breaches OPM recently reported have been particularly concerning to us because of the national security risk involved. According to testimony you

[525] June 9, 2015 DMAR at HOGR000092-93.
[526] U.S. Dep't of Homeland Security/US-CERT, Digital Media Analysis Report-465355 (June 9, 2015) at 000090 (US-CERT Production: Dec. 11, 2015).
[527] Saulsbury Tr. at 74-75.
[528] June 9, 2015 DMAR at HOGR0724-001154.
[529] U.S. Dep't of Homeland Security/US-CERT, Digital Media Analysis Report-465355 (June 9, 2015) at 000090 (US-CERT Production: Dec. 11, 2015).
[530] OPM Cybersecurity Events Timeline.

gave at a recent hearing on the OPM data breaches, the OPM personnel records that were compromised in one of those breaches were hosted in the data center maintained by the Department of Interior. Did the cyber attackers who gained access to those records also gain access to the Interior Department data center?

Ms. BURNS. So the adversary had access to our data center. It was exposed. There was no evidence based on the investigation that was led by DHS, US–CERT, and the FBI, there was no evidence that the adversary had compromised any other data aside from the OPM data.

Ms. KELLY. Okay, so the same cyber intruder who breached OPM's personal data, which the Department of Interior hosted on its servers, also breached the defense's of the Interior Department data center?

Ms. BURNS. So this, the intrusion that you're referring to, was a sophisticated breach. And my understanding, based on DHS' assessment, was that the adversary exploited, compromised credentials on OPM's side to move laterally and gain access to the Department of Interior's data center through a trusted connection between the two organizations.

Ms. KELLY. So the cyber intruder, did they gain access it to DOI's data center through OPM or was it the other way around?

Ms. BURNS. The adversary gained access to DOI's infrastructure through OPM, as far as I understand, based on DHS's investigation.

* * *

Ms. KELLY. In addition to hosting OPM's personnel records, the Department hosts data from other agencies in its data center. Is that correct? And, if so, which agencies?

Ms. BURNS. Yes. Actually, the Department is a—the data center in question, the biggest customer of the data center is actually Interior. So it's the Interior Business Center, what we call IBC. They're a shared service provider, and they are the majority user of the data center. And we also host some applications for the Office of the Secretary in the data center.[531]

The same day RAR files were being discovered (April 19, 2015), Protect also identified "command shells."[532] Command shells are significant because they provide a means for the attacker to remotely control a victim machine. On April 19, 2015, McClure wrote to Coulter:

---

[531] *Cybersecurity: The Department of the Interior: Hearing Before the Subcomm. on Information Tech. and Subcomm. on Interior of the H. Comm. on Oversight & Gov't Reform*, 114th Cong. 21-22 (July 15, 2015).
[532] McClure Tr. at 31; Email from Stuart McClure, Chief Exec. Officer, Cylance to Chris Coulter, Managing Dir., Cylance (Apr. 19, 2015, 9:01 p.m.), at CYLANCE_002112 (Cylance Production: Jan. 27, 2016).

"They quarantined one of the xCmd.exe files but I found two more. Might want to recommend they quarantine those too."[533] McClure explained the significance of finding "xCmd.exe files:"

> A. Sure. So XCMD -- so CMD stands for command, and they usually stand for command shells. And what that allows you to do is actually have remote access of their computer on your own computer. So **when you start XCMD on the victim box, it will then create a shell to you on your remote computer, wherever you are in the world, and you can then type commands as if you are sitting right there on the computer**.
>
> Q. And why did you recommend quarantining another two mentioned in the message?
>
> A. Because that's -- **that's as nasty as you can get. I mean, they can do anything that they want with that access**.[534]

Cylance and OPM made additional findings about the breach on April 19, 2015.[535]

Then on April 20, 2015, a Cylance expert contacted Coulter about OPM data collected and a "backdoor." Thus, began a chain of events eventually leading to the discovery background investigation data had been stolen. Specifically, the Cylance expert wrote to Coulter:

> Give me a call when you have some time. I'm going through the data now. Wanted to ask some questions about the system WCE was sitting on and a few others. You may want to have them get an image of [__] is **a backdoor that looks like the [command and control server] was active around 6/2014** corresponding to when they came out and said they had a problem. Callback was to resolved to if they have any kind of network or DNS logs going back that far.[536]

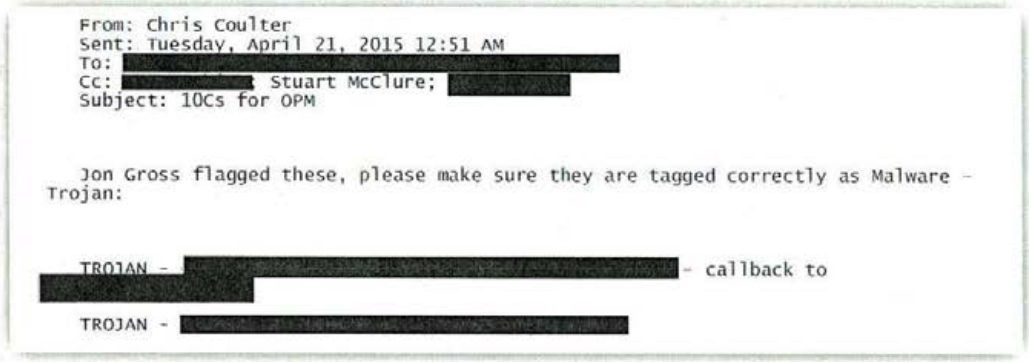
This communication in particular would start the process of revealing how the background investigation materials were compromised. More evidence would unfold and become clear in the coming days.

---

[533] McClure Tr. at 29; Email from Stuart McClure, Chief Exec. Officer, Cylance to Chris Coulter, Managing Dir. of Incident, Cylance (Apr. 19, 2015, 9:01 p.m.), at CYLANCE_002112 (Cylance Production: Jan. 27, 2016).
[534] McClure Tr. at 29-30.
[535] The same day that Cylance identified RAR files and was working to decode the passwords, Protect found "a fraudulent attempt at making this look like a Bit9 signed binary. See the signed by "Bit89 Inc."? And [website Virus Total] calls it quite evil." McClure Transcribed Interview, Ex. 10. VirusTotal, a subsidiary of Google, is a free online service that analyzes files and URLs enabling the identification of viruses, worms, Trojans and other kinds of malicious content detected by antivirus engines and website scanners. *About Virus Total*, VIRUS TOTAL available at: https://www.virustotal.com/en/about/.
[536] Coulter Tr., Ex. 6.

April 20-23, 2015 – More Key Trojans Identified; OIG First Notified.

The agency continued to expand its use of Protect through April 21, 2015. The tool was on 6,725 hosts and it was expected to roll out to 10,000 hosts soon thereafter.[537] On April 21, Cylance also identified two Trojans sitting on key servers.[538]



From: Chris Coulter
Sent: Tuesday, April 21, 2015 12:51 AM
To: [redacted]
Cc: [redacted] Stuart McClure; [redacted]
Subject: IOCs for OPM

Jon Gross flagged these, please make sure they are tagged correctly as Malware - Trojan:

TROJAN - [redacted] - callback to [redacted]

TROJAN - [redacted]

At that point, OPM also began utilizing more outside help. CyTech's CyFIR Enterprise was installed on the servers where Coulter had identified new pieces of Trojan malware.[539] CyTech's CyFIR then imaged malware and artifacts residing on these servers that were subsequently supplied to US-CERT. Those findings were covered in US-CERT's May 4, 2015 "Preliminary Digital Media Analysis Report" and June 9, 2015 "Digital Media Analysis Report."[540]

Cylance also discovered remnants of malware used by adversaries in the 2014 intrusion against OPM. CylanceProtect found "dormant" variants of Hikit, which was the primary malware used by the attackers discovered in 2014, on OPM's systems during the discovery phase of the 2015 investigation. Jeff Wagner, OPM's Director of IT Security Operations, stated Cylance. "In doing a full analysis of the entire network…did find an older version of Hikit. It also found library fragment files of malware."[541] Wagner testified regarding the Hikit malware found by Cylance and its relevance to the 2015 intrusion:

> A. So the Hikit variant discovered in 2015 was not an active piece of malware, it was a dormant piece of malware. That because Cylance was utilized to analyze the entire environment, we discovered the malware was dormant within one of the servers. It was believed to have been an abandoned piece of malware that was previously installed at some other time.
>
> Q. Was it related to the incident in 2015?

[537] McClure Tr., Ex. 11.
[538] Coulter Tr., Ex. 7.
[539] Briefing by U.S. Office of Pers. Mgmt. to H. Comm. on Oversight & Gov't Reform Staff (Apr. 18, 2016).
[540] U.S. Dep't of Homeland Security/US-CERT, Preliminary Digital Media Analysis Report - INC465355-A (May 4, 2015), at HOGR_US-CERT_000346-48 (US-CERT Production: Dec. 11, 2015); Briefing by U.S. Office of Pers. Mgmt. to H. Comm. on Oversight & Gov't Reform Staff (Apr. 18, 2016).
[541] Wagner Tr. at 126

A. We don't have direct evidence it was necessarily related to the 2015 incident. It was discovered in the 2015 incident.

* * *

Q. Sorry. So did you have any indirect evidence that the [Hikit] found referenced in the 2015 DMAR was at all involved in the 2014 breach?

A No. We don't believe…I don't remember the exact, quote, "born on date" of the malware, which shows the initial point of infection, but it was not during the 2015 timeframe of adversary activity. **So we really didn't have a recognized idea as to when it showed up**. It was one of those pieces of malware, as well as additional fragments of former malware that Cylance identified, and we proceeded to eliminate along with everything else.[542]

One of the two Trojans found on April 21 contained what US-CERT called a "unique"[543] file named winrsves.dll, with a compile time of 5:34:46 EST on March 18, 2011.[544] This file was a malicious Windows Dynamic Link Libraries (DLL) file designed to run as a service. When running, the DLL allows a hacker to pass and execute encrypted executables and DLLs to a victim system at will.[545]

This first "unique" Trojan file (winrsves.dll) contained a "plugin" framework that allowed it to import and load DLL files. US-CERT described the file as follows: "The DLL [which is identified as a Hikit Remote Access Tool (RAR)] is unpacked and loaded into memory, while never being written to disk. During execution, this DLL will attempt to read a configuration file in the same folder in which it was executed. This configuration is expected to have the same name as the originally executed file, but with a *.conf* extension. In this case, the expected configuration file is winrsves.conf. If this file is not found, the malware will create a configuration file which contains its default configuration."[546] The CMD.exe[547] Cylance found on April 19 would reveal that the configuration file contains the command and control location [redacted] The configuration file contains the configuration string [redacted][548]

---

[542] Wagner Tr. at 134-135

[543] U.S. Dep't of Homeland Security/US-CERT, Malware Analysis Report-460357-B (corrected) (April 24, 2015) at HOGR0724-001065 (OPM Production: Dec. 22, 2015).

[544] U.S. Dep't of Homeland Security/US-CERT, Preliminary Digital Media Analysis Report - INC465355-A (May 4, 2015), at HOGR_US-CERT_000348 (US-CERT Production: Dec. 11, 2015).

[545] U.S. Dep't of Homeland Security/US-CERT, Malware Analysis Report-460357-B (corrected) (April 24, 2015) at HOGR0724-001065 (OPM Production: Dec. 22, 2015).

[546] U.S. Dep't of Homeland Security/US-CERT, Malware Analysis Report-460357-A (April 24, 2015) at 000190 (US-CERT Production: Dec. 11, 2015).

[547] U.S. Dep't of Homeland Security/US-CERT, Malware Analysis Report-460357-A (April 24, 2015) at 000190-91 (US-CERT Production: Dec. 11, 2015).

[548] June 9, 2015 DMAR at HOGR0724-001154 (This particular HiKit uses the same strong [redacted]" in the output configuration file as US-CERT found in DMAR 355170).

The second Trojan was located on a server [redacted] and was called "[redacted]." According to US-CERT this was a *Dropper.Generic9.TIC* Hikit found to have resided on the victim machine since September 15, 2012 at 07:07:53AM.[549] This binary also pointed to the malicious domain [redacted]"[550] The cybersecurity event that was developing at OPM was serious. It was not until April 22, 2015, however, that the agency notified the Office of the Inspector General that it was dealing with a breach.[551] In fact, the notification occurred entirely by accident.[552]

And while the Protect deployment was successfully identifying critical malicious items, the product was still being introduced into OPM's system conservatively. Protect was in Alert mode meaning threats were not automatically quarantined.[553] In addition, Protect was not yet on all OPM hosts. On April 23, 2015, Coulter emailed an OPM official: "Just letting you know we do not have Protect on the following key hosts [servers]."[554]

April 24-25, 2015 – OPM Upgrades Protect to Auto-Quarantine Mode.

On April 24, 2015, OPM upgraded Protect to auto-quarantine mode. At 4:11 p.m. on April 24, Coulter emailed several colleagues to announce the upgrade. He wrote:

> Guys - OPM hit critical mass today and **is burning the house** - literally! **They just hit 'global-quarantine' for every threat! I think it was around 1180 threats in the queue. This was done per senior orders**. They are also pulling the power on every device starting Saturday at 9am - Sunday at 5pm. I need everyone's help to make sure what they quarantined will not be mission critical files. I have been up for 24 hours so I really do need help.[555]

> On Apr 24, 2015, at 4:11 PM, Chris Coulter [redacted] wrote:
>
> Guys - OPM hit critical mass today and is burning the house - literally!
>
> They just hit "global-quarantine" for every threat! I think it was around 1180 threats in the queue. This was done per senior orders.
>
> They are also pulling the power on every device starting Saturday at 9am - Sunday at 5pm.
>
> I need everyone's help to make sure what they quarantined will not be mission critical files. I have been up for 24 hours so I really do need help.
>

[549] June 9, 2015 DMAR at HOGR0724-001173.
[550] *Id.*
[551] OIG Memo, *Serious Concerns*.
[552] *See Infra*, Chapter 7: OPM's CIO and its Federal Watchdog.
[553] McClure Tr. at 33.
[554] Coulter Tr., Ex. 8.
[555] McClure Tr., Ex. 12.

Prior to April 24, OPM manually considered whether each item that Protect flagged should be removed from the system. McClure testified:

> My recollection was [OPM was] processing all the alerts themselves, along with the help of us at Cylance, our alert management team, as well as Chris Coulter, myself and others, to help them triage and process the alerts to make sure that they are malicious and not safe, and just trying to empower OPM themselves to make the judgment call on whether to quarantine those files and move them out of alert-only.[556]

Thus, while Protect was operating in alert mode, the burden was on OPM staff to determine what files should be quarantined, or be allowed to remain operational in OPM's environment. McClure testified:

> Q. Can you define, when you said that OPM was processing things on their own, can you define "processing"?
>
> A. Yes. They were in our management console looking at each alert trying to understand if they should actually quarantine it, delete it, or just allow it to continue to be on the system and study it for whatever purpose.
>
> Q. So OPM was making the decision on what to delete out of the items identified prior to April 24th, 2015?
>
> A. Correct. All customers manage their own quarantine.[557]

Saulsbury, who was on site at OPM on April 24, 2015, provided similar testimony:

> So after we observed that Cylance V was able to detect the APT malware, in this case it was, in the 2015 incident it as a malware family called PlugX. And once we were able to determine that V was able to detect PlugX, at some point there was a decision made to deploy the Protect agent to all of OPM's machines.
>
> So that was done with the assistance of the vendor of Cylance. And so the guy that I am emailing on that is Chris Coulter. So Chris was really good about helping us getting Protect deployed throughout the environment and then also analyzing all the findings that it is coming back with. So Cylance is detecting not just the APT malware, but every type of malicious, like, adware toolbar that somebody downloads and things like that, as well as the false positives here and there.

---

[556] McClure Tr. at 34-35.
[557] McClure Tr. at 35-36.

> So Chris was really good about helping us triage through that list and separate what we want to quarantine versus what is false positive and whitelisted. So at a certain point we were confident enough that we had identified all of the malware and had whitelisted the business critical applications that needed to be whitelisted. And so Jeff instructed us to quarantine all of the identified findings.
>
> What that quarantine means is, so when Cylance detects something, we just had it in alert mode. **So it would see it and say, hey, this is bad, but it is just alerting us on it, it is not actually doing anything about it. So what we essentially did on April 24th was press a button in the Cylance console and says everything that you've seen that is bad, take that and quarantine it so it is not operable on the machine.**[558]

Wagner also confirmed that OPM quarantined all the identified malware on or about April 24, 2015. With respect to why the quarantine did not happen before April 24, 2015, Wagner stated:

> So once you identify malware functionality or adversary activity, you try to get a sense of the adversary's intention, activities, and exposure. You look to see how deep they are in the environment. So once you discover something on the 15th, we didn't want to just start shutting things off.
>
> We didn't understand the depth in which the adversary had been in the environment. With the deployment of the Cylance tool, a full accountability of all binaries, we had discovered, identified, and all the malware was placed into the quarantine queue by I think it was the 19th of April . . . . And by the 24th, we had a full understanding that it had discovered everything that was to be discovered, and we no longer necessarily needed the adversary to have an active presence within the environment. So we ordered Cylance to destroy the malware.[559]

The auto-quarantine did not apply to all of OPM's systems, however. For certain systems, OPM made a value judgment as to whether they should be included in the auto-quarantine, or remain subject to the human command quarantine in auto-alert mode. Coulter provided guidance to his colleagues at Cylance on April 24, 2015 regarding what files to quarantine. He wrote:

> I would say anything on desktops are ok to quarantine. Servers should be the only thing questioned at this point. If they can live without it keep it blocked. They are setting up some help desk protocols to identify issues that come out of this.
>
> Mission critical items that I know of:

[558] Saulsbury Tr. at 72-73.
[559] Wagner Tr. at 121-122.

> USA JOBS related apps - **they said if we bring that down senators will come for us**
>
> LAN Desk / SCCM
>
> SQL/Oracle components and connectors to mainframes
>
> Past that they can live without for a few weeks. This is a desperate move, tomorrow is even more desperate by unplugging every device and moving over to new networks. They will blame any issues on the power outage ;).[560]

McClure testified that in auto-quarantine mode, mission-critical items may stay in "alert" mode so as not to undermine the system in the event of a false positive.[561] McClure also testified that OPM should have considered shutting down mission-critical items given the severity of what Cylance was finding. He testified, "Yes, they should be."[562]

Documents and testimony show OPM used Protect as its quarantine tool and that Protect was not put into auto-quarantine mode until April 24, 2015. Documents and testimony also show some OPM systems were not placed into auto-quarantine mode at all. Contrary to this evidence, OPM's leadership testified before the Committee in June 2015 that the quarantine was fully in place by an earlier date, and stated that the malware was "latent" and merely being observed.[563] The term "latent" means the malware is not active on the environment—it is frozen or otherwise not running on active computer processes. The quarantine status was not activated until April 24, 2015 when OPM gave Cylance the authority to place Protect into auto-quarantine mode.[564] Unless Protect is in "auto-quarantine" mode, malicious items are not latent—an action is required to stop malicious items from functioning in the environment.[565]

April 26 – April 30, 2015: First Signs of Lost Background Materials

According to Wagner, in the days that followed the deployment of Protect's auto-quarantine function, OPM had "discovered everything that was to be discovered,"[566] but significant discoveries continued. The new discoveries were noteworthy because they provided evidence related to the loss of background investigation materials.

On April 26, 2015, Coulter and Jonathan Tonda (an OPM contractor at the time in OPM IT Security Operations) engaged in an email exchange about a segment of the OPM network.[567] This was the same segment that a Cylance expert asked Coulter to image on April 20 writing: "Give me a call when you have some time. I'm going through the data now. Wanted to ask some

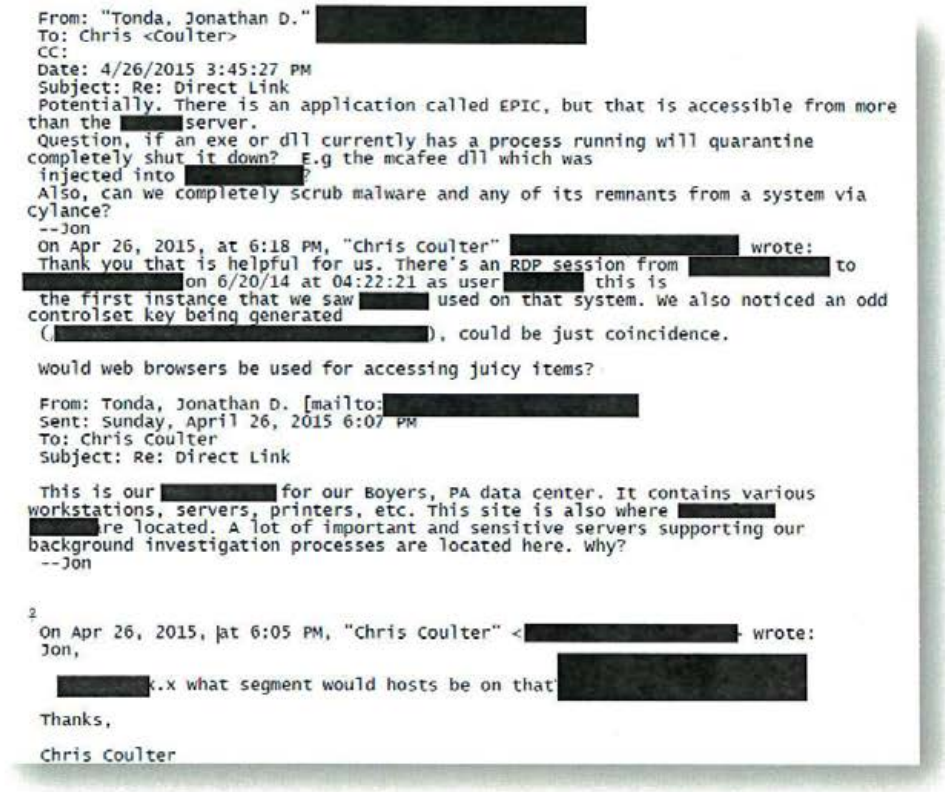
---

[560] Coulter Tr., Ex. 17.
[561] McClure Tr. at 67.
[562] McClure Tr. at 68.
[563] *Hearing on OPM Data Breach: Part II* at 69; *see Infra,* Chapter 5: The CyTech Story for more on quarantine statements by OPM officials before the Committee.
[564] McClure Tr., Ex. 12; Coulter Tr. at 74-75.
[565] McClure Tr. at 34-36; Coulter Tr. at 34-36.
[566] Wagner Tr. at 121-122.
[567] Coulter Tr. Ex. 18.

questions about the system WCE was sitting on and a few others. You may want to have them get an image of [__] is **a backdoor that looks like the [command and control server] was active around 6/2014 corresponding to when they came out and said they had a problem.** Callback was to resolved to if they have any kind of network or [Domain Name System] logs going back that far."[568]

In this April 26 email exchange between Coulter and Tonda, Coulter was investigating a Remote Desktop Protocol (RDP) session that dated back to June 20, 2014 and accessed a particular segment of OPM's environment. Coulter asked Tonda what was hosted on the segment Coulter was investigating.[569] Tonda responded the segment Cylance identified was where ". . . [a] lot of important and sensitive servers supporting our background investigation processes are located."[570] **This was an important development because this server provided access to the PIPS mainframe – where background investigation data was stored.**[571] US-CERT/OPM would later confirm the "first known adversarial access to OPM's mainframe" as occurring June 23, 2014.[572]

[568] Coulter Tr., Ex. 6.
[569] Coulter Tr. Ex. 18.
[570] *Id.*
[571] Coulter explained in the email that the segment he had identified was a key "jump box" at OPM identified as [redacted] – a jumpbox means a server that manages access between two different network sections of the larger information technology environment (Saulsbury Tr. at 74-76). At OPM, this particular jumpbox enabled access to various parts of the OPM environment (Saulsbury Tr. at 74-76) and Cylance's Coulter was letting OPM know on April 26 that the jumpbox had a Remote Desktop Protocol (RDP) session to a significant server [redacted] that gave access to the portion of OPM's network where background investigations are stored (Coulter Tr., Ex. 18).
[572] Briefing by US-CERT to H. Comm. on Oversight & Gov't Reform Staff (Feb. 19, 2016); OPM Cybersecurity Events Timeline.



From: "Tonda, Jonathan D." [redacted]
To: Chris <Coulter>
CC:
Date: 4/26/2015 3:45:27 PM
Subject: Re: Direct Link
Potentially. There is an application called EPIC, but that is accessible from more than the [redacted] server.
Question, if an exe or dll currently has a process running will quarantine completely shut it down? E.g the mcafee dll which was injected into [redacted]?
Also, can we completely scrub malware and any of its remnants from a system via Cylance?
--Jon
On Apr 26, 2015, at 6:18 PM, "Chris Coulter" [redacted] wrote:
Thank you that is helpful for us. There's an RDP session from [redacted] to [redacted] on 6/20/14 at 04:22:21 as user [redacted] this is the first instance that we saw [redacted] used on that system. We also noticed an odd controlset key being generated ([redacted]), could be just coincidence.

Would web browsers be used for accessing juicy items?

From: Tonda, Jonathan D. [mailto:[redacted]
Sent: Sunday, April 26, 2015 6:07 PM
To: Chris Coulter
Subject: Re: Direct Link

This is our [redacted] for our Boyers, PA data center. It contains various workstations, servers, printers, etc. This site is also where [redacted] are located. A lot of important and sensitive servers supporting our background investigation processes are located here. Why?
--Jon

2
On Apr 26, 2015, at 6:05 PM, "Chris Coulter" <[redacted]> wrote:
Jon,

[redacted].x what segment would hosts be on that [redacted]

Thanks,

Chris Coulter

With respect to this jump box, US-CERT found another related directory infected with PlugX. US-CERT reported:

> Malicious binaries no longer reside on the victim machine, which has been identified as a jump server; however, analysis displays the system was once infected by malware. Remnants of malicious files were found in the directory [redacted] with PlugX files [redacted], [redacted], [redacted] and [redacted] located on image. Also metadata displays malicious domain opmsecurity[.]org found on image.[573]

As was the case with the McAfeeSVC directory that contained malware, this directory—[redacted]—contained four files: one output keylogger file; an innocuous file that PlugX used; and two binaries that were PlugX malware files.[574]

By the end of April, the situation at OPM began to stabilize and Cylance personnel prepared to leave the agency's headquarters. On April 29, 2015, Cylance reported to Wagner and others at OPM that "I will be working remote today as I think everything is resolved that would have required me to be onsite."[575]

---

[573] June 9, 2015 DMAR at HOGR0724-001155.
[574] June 9, 2015 DMAR at HOGR0724-001154.
[575] Coulter Tr., Ex. 14.

As part of a close out email, Coulter updated on the work that Protect was doing. Coulter wrote: "We have been working diligently to permanently assign new threats into either blacklist or safe[-]list que. There [are] roughly 225 files that I would like to go over before we take any action. I will send the spreadsheet of these tonight.[576]

Cylance also provided instructions to other entities who were remaining on site at OPM. Coulter wrote:

> If OPM can commit to having all output script results back before Thursday next week this plan will work. I will have 2 of my best guys scheduled to come down Thursday and Friday next week to help in analyzing the results of the *.bat script deployments. We will be done on Friday around [Close of Business] and would like to have a formal meeting with the CyFir & the other team members to close out.[577]

While the situation appeared to be contained, OPM continued to face new and evolving threats. For example, on May 1, 2015, Coulter wrote Wagner and Tonda: ". . . we just saw the very first instance of a prevented Upatre/Dyre Trojan infection (due to setting auto-quarantine). Completely unknown to industry and stopped before it could do any harm."[578]

The Decision to Purchase CylanceProtect

CylanceProtect was the first tool that OPM used after the agency learned its network was compromised, and the tool immediately found malware and set about cleaning OPM's enterprise. This raises a question as to why OPM did not purchase and deploy the tool sooner, in June 2014, when it may have been able to prevent or mitigate the attack, especially given the fact that OPM knew its most sensitive data was being targeted by sophisticated hackers. Documents and testimony show internal agency politics and procurement challenges made it difficult to quickly purchase and deploy security tools.

Political Challenges on the Desktop

On June 12, 2014, less than three months after becoming aware of a significant cyberattack, OPM executed a Cylance product evaluation agreement allowing OPM to test the functionality of both V and Protect for a limited period of time.[579] McClure testified that Cylance's demonstrations typically last 30-60 days, and in "rare exceptions" extend to 90 days.[580] With respect to why OPM was considering their products, McClure stated: "It had been communicated to me through [Cylance staff] that [OPM] had a specific use case or potential problem, that they wanted to test new technology that might be able to help them."[581] However, OPM delayed a decision about acquiring either product for months, even after key officials knew

---

[576] Coulter Tr., Ex. 14.
[577] *Id.*
[578] Coulter Tr., Ex. 22.
[579] McClure Tr., Ex. 2.
[580] McClure Tr. at 15.
[581] McClure Tr. at 13.

the agency was under attack and despite allocating resources to procure tools to secure OPM's legacy IT environment.[582]

After the March 2014 data breach, OPM's OCIO launched a multi-phased project that included buying security tools to secure the legacy IT environment and create a new IT environment.[583] In June 2014, OPM made a sole-source award to a contractor called Imperatis for this project and CIO Seymour was designed as the OPM official to manage the contract.[584] The estimated cost of the initial project phases was $93 million and $18 million was allocated immediately with the June 2014 award.[585] The first phase of this contract (referred to as the tactical phase) was focused on purchasing security tools for the legacy IT environment to strengthen OPM's legacy systems, but Cylance does not appear to have been considered as part of this contract despite the immediate need for tools like Cylance.

Separately and three months after initially viewing Cylance's products OPM decided to purchase one Cylance product for use in its legacy system on September 27, 2014. The agency opted to purchase V, which is the product limited in scope when compared to Protect, and that did not provide preventative capabilities.[586] This decision was made despite the fact that information security personnel within OPM wanted to acquire Protect, because they recognized its potential to detect threats.[587]

Brendon Saulsbury, a contractor in OPM's IT Security Operations, testified:

> I believe [Cylance Protect] [is] very useful. The fact that they do heuristics-based analysis as opposed to signature-based was beneficial in that they are able to detect our APT malware, which was undetectable at the time by traditional signature-based antivirus tools."[588]

Saulsbury testified he shared that impression of Cylance's products in 2014, long before OPM was in crisis mode, and that he communicated that belief to his managers.[589]

---

[582] By the end of June 2014, agency officials received US-CERT's final incident report – which made clear that sophisticated attackers were working to acquire information related to the PIPS system. *See* June 2014 OPM Incident Report. OPM was also keenly aware of other deficiencies in its system by this time that it needed to address, such as the OPM Inspector General warning the agency in its fiscal year 2013 FISMA audit that problems in its information systems constituted a "material weakness." *See* Office of Inspector Gen., U.S. Office of Pers. Mgmt., Report No. 4A-CI-00-13-021, *Federal Information Security Management Act Final Audit FY 2013*, at ii (Nov. 21, 2013) available at: https://www.opm.gov/our-inspector-general/reports/2013/federal-information-security-management-act-audit-fy-2013-4a-ci-00-13-021.pdf..

[583] *OPM Data Breach: Hearing Before the H. Comm. on Oversight & Gov't Reform*, 114th Cong. (June 24, 2015) (testimony of Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt.); *see Infra* Chapter 8 for more on the IT Infrastructure Improvement project and contract.

[584] Imperatis Letter Contract (June 16, 2014), Attach. 1 at 000003 (Imperatis Production: Sept. 1, 2015); *Id.* at 000013 (designating Seymour as the contracting officer representative).

[585] *OPM Data Breach: Hearing before the H. Comm. on Oversight & Gov't Reform*, 114th Cong. (June 16, 2015) (testimony of Donna Seymour, Chief Information Office, Offiice of Personnel Mgmt.); Imperatis Letter Contract (June 16, 2014) Attach. 1 at 000006 (Imperatis Production: Sept. 1, 2015).

[586] McClure Tr., Ex. 3.

[587] Wagner Tr. at 91-92.

[588] Saulsbury Tr. at 67-68.

[589] Saulsbury Tr. at 66-68.

Documents and testimony show internal politics contributed to OPM's inability to swiftly purchase the tool that its IT security personnel wanted to acquire, specifically "political challenges on the desktop" at the agency.[590] With respect to the meaning of that term, and why it would have prevented OPM from acquiring Protect in 2014, McClure testified:

> Typically in larger environments, there are other people that own the desktop. So security people don't own the desktop. Security people make recommendations to the desktop teams: You got to do this. You got to do that. You got to install this. You got to install that. And the desktop preparations people usually come from the IT side, the information technology side of the house, versus the security side that usually tries to come outside of the IT to be sort of the watch guard of IT and make sure that what they're doing is secure.
>
> So there's always a firewall, unfortunately, between them, virtually, between the IT guys that try and own the desktop and run the desktop and the security guys who just want the thing to be secure.
>
> Because IT's priorities are around availability predominately, not always confidentiality or integrity, and security is all about confidentiality, integrity, and things like that, so that becomes, unfortunately, a challenge between those organizations. And unless they report separately all the way up to the top, it's always going to favor the folks that own the desktop. The decision-making, the way that they go about trying to find solutions and what they deploy, they control the desktop; they own the desktop, so ultimately they have the last word on what gets installed.[591]

McClure testified:

> [A]necdotally what I have been told was that they had had challenges getting this installed on the endpoint, on the desktop during that initial timeframe in 2014. So because of that, they purchase[d] -- they could only purchase V, which is just this detection product. And I had been told that they were not happy with having to only buy V, that they really wanted to buy PROTECT.[592]

McClure testified these "political challenges"[593] prevented OPM from acquiring Protect, and that had the product been acquired, "It would have prevented this attack."[594]

---

[590] McClure Tr., Ex. 4.
[591] McClure Tr. at 44-45.
[592] *Id.*
[593] McClure Tr. at 16-17.
[594] McClure Tr. at 16-18.

Counterpoint – Lack of FedRAMP Compliance

OPM's Director of IT Security Operations, Jeff Wagner, testified that political reasons were not why OPM failed to purchase Protect. Wagner stated the primary reason that OPM did not acquire Protect was because "Cylance didn't currently have a FedRAMP-certified cloud."[595]

The Federal Risk Authorization Management Program, or "FedRAMP," is a federal government program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.[596] A December 2011 guidance memo issued by the OMB defines the requirements for executive departments and agencies using FedRAMP in the acquisition of cloud services.[597]

Wagner testified that OPM "…had the capability of deploying the Protect tool. We just didn't – because of the FedRAMP issue, **we felt it wasn't necessarily critical at the moment**. It would have been a risk deploying it to a non-fed ramp environment."[598] While Wagner acknowledged that Protect "doesn't necessarily upload sensitive data or PII data or anything of that nature," he testified that a lack of FedRamp authorization was the primary reason for not securing the tool. Wagner testified: "**In a perfect world, we would have deployed it earlier, but because we were trying not to break rules and trying to live within structures, correct, we didn't deploy it.**"[599]

Wagner's assertion that the reason OPM did not buy Cylance tools was because they were not FedRAMP complaint is not supported by the facts. The fact is that OPM ultimately deployed and purchased CylanceProtect without being FedRamp compliant. Protect was not FedRamp compliant when it was first deployed throughout OPM's enterprise on April 17, 2015[600] and it was not FedRamp compliant when it was ultimately purchased in June 30, 2015.[601] **In other words, OPM swiftly broke the rules once its house was already burning down, but not when it was in a position to save it.**

Further, at the same time OPM apparently declined to purchase Protect because it was not FedRAMP compliant, OPM *did purchase V* which was a cloud-based product and not FedRAMP

---

[595] Wagner Tr. at 91-92. Wagner also said that funding contributed to the decision. However, the funding ultimately obligated to CylanceProtect was a mere fraction of what OPM began immediately spending to build out a new infrastructure. In late October 2015, OPM reported to the Committee that it had spent an estimated $60 million in FY2014 and FY2015 for the new IT infrastructure project. About 80 percent of the funds originated from OPM's revolving fund and the remaining 20 percent from a variety of discretionary and mandatory funds areas. Email from U.S. Office of Pers. Mgmt. to H. Comm. on Oversight & Gov't Reform Staff (Oct. 28, 2015) (on file with Committee).

[596] To learn more about FedRAMP, visit: https://www.fedramp.gov/.

[597] Memorandum from Office of Mgmt and Budget, Exec. Office of the President, to Chief Info. Officers, *Security Authorization of Information Systems in Cloud Computing Environments* (Dec. 8, 2011), https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fedrampmemo.pdf.

[598] Wagner Tr. at 112.

[599] Wagner Tr. at 144.

[600] McClure Tr. at 23.

[601] Telephone Interview with Stuart McClure, Chief Exec. Officer, Cylance (Feb. 18, 2016). *See also* Cylance Purchase Order from Assurance Data, Inc. (June 30, 2015) at CYLANCE _000018 (Cylance Production: Dec. 17, 2015).

compliant at the time. OPM purchased V on September 27, 2014, and the invoice covers Cylance Infinity API, which is the application programming interface for V. Cylance V has both a local- and cloud model.[602] McClure stated: "the V model . . . was cloud-based and local-based."[603]

FedRAMP compliance is an important part of federal agencies' efforts to ensure security and realize efficiencies with cloud-based products. In the case of OPM, however, its compliance efforts were inconsistent when acquiring tools. The agency did not comply with FedRAMP requirements when it purchased Cylance's non-FedRAMP compliant V. Then a mere six months after OPM declined to purchase Protect, OPM asked Cylance for another demonstration of Protect (in the spring of 2015), while the product was still not FedRAMP compliant. On March 20, 2015, OPM executed a clickwrap evaluation agreement that McClure testified is "our internal process for managing somebody that's evaluating our software, so that it doesn't stay in evaluation mode forever. . . So since [OPM] had disengaged on the Protect side the prior year at a certain point, they had come back and said they wanted to retest, so we re-engaged with them through that process."[604] In other words, OPM's interest in Protect did not diminish with time despite the lack of FedRamp compliance. Then after OPM had been breached – OPM deployed Protect – which again was not (at the time) FedRAMP compliant.

OPM ultimately deployed Protect in April 2015, once the agency was in crisis mode, despite its lack of FedRAMP compliance. Director of IT Security Operations Jeff Wagner testified that OPM took this action because "Protect was able to find malware that nothing else could" and he acknowledged that he would have purchased Protect earlier had he been able. He stated:

> Q. So since they didn't have a FedRAMP-certified cloud that would meet all the Federal requirements, we felt it would be less than optimal to go with the PROTECT right away.
>
> A. Cylance was in the process of getting a FedRAMP cloud, and we thought we'd utilize the V as much as we could until they got to that point. I think they're still working to get FedRAMP certified; however, we moved to utilize the PROTECT because it was able to find malware that nothing else could.
>
> Q. Is it fair to say that if it was up to you, you would have gotten PROTECT at the earliest convenience?
>
> A. Absolutely.[605]

The agency purchased Protect on June 30, 2015 when it was still had not been deemed FedRAMP compliant.[606] As of June 2016, Cylance's application is "FedRAMP in Process"[607],

---

[602] McClure Tr. at 16.
[603] *Id.*
[604] McClure Tr. at 19-20.
[605] Wagner Tr. at 91-92.

with OMP acting as Cylance's sponsor.[608] It is not known why OPM did not pursue a similar sponsorship path in June 2014.

In sum, Wagner's assertion that OPM did not deploy Cylance's preventative tool – Protect – sooner because it was not FedRAMP compliant is lacking given OPM's actions at the time in buying other non-FedRAMP compliant products.

OPM Purchases Protect After Nearly Losing Access to It

Despite Cylance's significant support to OPM in April through May 2015 following discovery of the attack, OPM was slow to execute payment for services rendered,[609] or execute a purchase agreement for Protect. In addition, OPM and their contractor responsible for building the new IT infrastructure was reticent to consider Cylance tools – despite their proven record during the 2015 incident response period.

OPM's contractor Imperatis, which was responsible for building out the new IT infrastructure, asked Cylance on May 12, 2015 to conduct a demonstration in order to be considered as a security tool for the new IT infrastructure.[610]

From: Nicholas Warner [redacted]
Sent: 5/12/2015 9:35:09 PM
To: Matt Morrison [redacted]
CC: [redacted]
Subject: Fwd: Cylance Info and meeting request for OPM Shell

A demo? Really?

NW

Begin forwarded message:
From: Patrick Mulvaney <[redacted]
Date: May 12, 2015 at 1:39:23 PM PDT
To: Matthew Morrison <[redacted]
Cc: [redacted] 'Nick Warner [redacted]
Subject: RE: Cylance Info and meeting request for OPM Shell
We can possibly take a look although it may be a couple weeks out, we have all of our engineers engaged with other vendor installs at the moment, and are on a tight schedule.
If you could reach back out in 2 weeks, we can assess where our bandwidth is at to support a demo, in the meantime I have sent the information out to my team.

---

[606] McClure Tr., Ex. 1; *see also* Cylance Purchase Order from Assurance Data, Inc. (June 30, 2015) at CYLANCE 000018 (Cylance Production: Dec. 17, 2015).
[607] FedRamp, Cylance, Inc. – CylancePROTECT, https://marketplace.fedramp.gov/index.html#/product/cylanceprotect?sort=productName (Last accessed 090216).
[608] *Id.*
[609] McClure Tr. at 85. (McClure testified that "If I recall, I think it took about 4 or 5 months to get fully paid.").
[610] Coulter Tr., Ex. 23.

The documents show Cylance employees were surprised by the way OPM was handling the procurement process. On June 22, 2015, Cylance CEO McClure emailed a business partner:

> I am having flashbacks to OPM one year ago when they couldn't pull the trigger on Protect because of political challenges on the desktop, so instead only bought V which is detection only. So of course, it didn't prevent the hack they just suffered through, it only notified them after the fact. Then, we installed Protect a year later, in April of this year, and it detected, cleaned and is preventing new attacks every day there. Jeff [Wagner] is kicking himself that he didn't deploy us when 'there wasn't an imminent threat.'[611]

OPM was also slow to ensure they could maintain access to Protect and eventually purchase this tool. On June 30, 2015, Cylance warned CIO Donna Seymour that the agency would lose access to Protect that evening, because the demonstration status was ending and no purchase had been made.

From: Seymour, Donna K. [mailto:[redacted]
Sent: Tuesday, June 30, 2015 3:23 PM
To: Stuart McClure
Subject: RE: Important: Extending your CylanceProtect Evaluation @ OPM

Stuart, Thank you for contacting me. I am getting some intel on this situation now and someone will be in touch with you soonest.

Take care,
Donna

From: Stuart McClure []
Sent: Tuesday, June 30, 2015 4:25 PM
To: Seymour, Donna K.
Subject: Important: Extending your CylanceProtect Evaluation @ OPM

Donna,

In the interest of national security, and understanding the gravity of the situation you are dealing with, can we please get on the phone
today to discuss extending your CylanceProtect deployment evaluation which began on 4/17/2015.

The evaluation is scheduled to end tonight at midnight PST, after 74 days of deployment to over 10,250 devices where we've
detected and blocked almost 2,000 pieces of malware (including the critical samples related to your breach), which were completely
missed with your prior protection technologies.

Please let me know if/when we can jump on a call today/tonight.

Thanks,

Stuart McClure

[611] Email from Stuart McClure, Chief Exec. Officer, Cylance to [redacted] (June 22, 2015, 7:49 a.m.) at CYLANCE_001769 (Cylance Production: Jan. 27, 2016).

McClure wrote to Seymour: "The evaluation is scheduled to end tonight at midnight PST, after 74 days of deployment to over 10,250 devices where we've detected and blocked almost 2,000 pieces of malware (including the critical samples related to your breach), which were completely missed with your prior protection technologies."[612]

Seymour responded: "Thank you for contacting me. I am getting some intel on this situation now and someone will be in touch with you soonest."[613] In July 2015, OPM finally purchased a perpetual license for Protect and access to one year of support and update services that must be renewed on an annual basis (where the initial support services will expire in September 2016). The agency, while now current in payments to the vendor, took four-to-five months to compensate Cylance for its product and work provided.[614]

The significance of the cutting edge preventative technology offered by Cylance in responding to the OPM data breach cannot be overstated. Wagner testified as to why OPM did not find the 2015 attacker, who accessed OPM's system as early as May 7, 2014, prior to the "Big Bang." Wagner cited the fact that OPM did not have a tool like the one Cylance provided. He stated:

> Q. Is it possible that FBI, DHS, and the other folks that were advising you in 2014, that they were unable to detect a latent malware or other parts of that foothold in other directories or portions of the network?
>
> A. Once again, the detection of malware prior to a tool like Cylance is based on what you know. So it's very plausible that there would be instances in which detection would go unnoticed, because you have to know what you're looking for to find it.[615]

Perhaps most importantly, given documents that demonstrate the tool's effectiveness, Cylance would have likely been able to find variants of the malware already on OPM's system in early June 2014 and prevented further compromise. Given that the attackers did not appear to move laterally into the background investigation system until June 23, 2014, if OPM had used CylanceProtect in early June 2014, there is a distinct possibility the exfiltration of data, such as the background investigation data could have potentially prevented and/or the data losses incurred in the fall and early 2015 could have been mitigated.

The Committee obtained documents that show federal agencies are facing a dilemma. On June 18, 2015, the *Washington Post* published a story in which government officials described the challenges that agencies deal with when purchasing cyber technologies.[616] The story stated: "But one challenge was a bureaucracy that made it difficult to buy security tools quickly,

---

[612] McClure Tr., Ex. 20.
[613] *Id.*
[614] McClure Tr., at 85-86.
[615] Coulter Tr. at 139.
[616] Ellen Nakashima, *Officials: Chinese Had Access to U.S. Security Clearance Data for One Year,* WASH. POST, June 18, 2016, available at: https://www.washingtonpost.com/news/federal-eye/wp/2015/06/18/officials-chinese-had-access-to-u-s-security-clearance-data-for-one-year/ /

officials said. 'OPM can't get through government procurement that fast,' said a U.S. official, who was not authorized to speak for the record."[617]

The Committee obtained an internal OPM email that shows OPM's Director of IT Security Operations Jeff Wagner was the anonymous "U.S. official" quoted in the story. The email from Wagner to the *Washington Post* reporter regarding OPM's acquisition of tools following the breach identified in March 2014 stated:

> The following month, in March 2014, the Department of Homeland Security notified OPM of the first hack of the security clearance database. In May that year, the agency did a 'remediation Big Bang,' Wagner said, to try to make improvements to the system. But one challenge was a bureaucracy that made it difficult to buy security tools quickly, he said. 'I can't get through government procurement that fast,' Wagner said. He noted an Office of Inspector General audit suggested 'we were breaking rules by failing to have key systems certified. 'Well, I couldn't go any faster without breaking [procurement] rules.'[618]

The documents and testimony show OPM's IT security personnel identified tools they believed would make the agency's enterprise more secure and failed to purchase and deploy the most effective and cutting edge preventative technology. As the record demonstrates, the Cylance tools later proved invaluable after 74 days of deployment to over 10,000 devices these tools detected almost 2000 pieces of malware on OPM's system and later blocked new threats. Unfortunately, the most effective preventative tool – Protect was not deployed until long after the attackers stole background investigation and fingerprint data and personnel records from OPM's system. The next Chapter describes the assistance another contractor provided to OPM during the 2015 incident response period.

---

[617] *Id.*

[618] Email from Press Secretary, U.S. Office of Pers. Mgmt., to Jeff Wagner, Dir. Info. Tech. Security Operations, U.S. Office of Pers. Mgmt. (June 18, 2015, 8:01 p.m.), at HOGR 020316-000266-67 (OPM Production: Feb. 16, 2016).

Chapter 5: The CyTech Story

On June 10, 2015, the *Wall Street Journal* reported "four people familiar with the investigation said the [OPM] breach was actually discovered during a mid-April sales demonstration at OPM by a Virginia company called CyTech Services, Inc. which has a network forensics platform called CyFIR."[619] The agency, on the other hand, issued a press release that said the breach was discovered as a result of an "aggressive effort to update its cybersecurity posture, adding numerous tools and capabilities to its networks . . . in April 2015, OPM detected a cyber-intrusion affecting its information technology systems and data."[620]

The Committee has investigated the seemingly conflicting statements and as is often the case, the truth is somewhere in between and the story more complicated than it appears. The documents and testimony do not definitively resolve this dispute. They do, however, support the following findings:

1. CyTech, a service disabled veteran-owned small business contractor, participated in several meetings with OPM in early 2015 to discuss the capabilities of their CyTech Forensics and Incident response (CyFIR) tool and to provide a demonstration of their CyFIR tool on April 21, 2015 at OPM headquarters.

2. During CyTech's April 21, 2015 demonstration, CyTech identified or "discovered" malware on the live OPM IT environment related to the incident. There is no evidence showing CyTech was aware at the time of the April 21 demonstration that on April 15 OPM had reported to US-CERT an unknown Secure Sockets Layer (SSL) certificate beaconing to a unknown site (opmsecurity.org), which was an initial indicator of compromise related to the background investigation data breach.[621] The record confirms the agency reported this finding to US-CERT on April 15, 2015.[622] Further, there is no evidence CyTech was aware that OPM (in consultation with Cylance) deployed CylanceV on April 16 and then deployed CylanceProtect on April 17, both of which identified additional key malware samples related to the breach.[623]

3. Beginning on April 22, 2015, CyTech offered and began providing significant incident response and forensic support to OPM related to the 2015 incident. The documents and testimony show OPM and Cylance recognized CyFIR's ability to quickly obtain forensic images. CyTech provided an expert to manage the CyFIR tool and continued to provide onsite support through May 1, 2015. CyTech was not paid for those services.

---

[619] Damian Paletta & Siobhan Hughes, *U.S. Spy Agencies Join Probe of Personnel-Records Theft*, WALL STREET JOURNAL, June 10, 2015, http://www.wsj.com/articles/u-s-spy-agencies-join-probe-of-personnel-records-theft-1433936969.

[620] U.S. Office of Personnel Management, Press Release, *OPM to Notify Employees of Cybersecurity Incident* (June 4, 2015).

[621] AAR Timeline – Unknown SSL Certificate (April 15, 2015), at HOGR020316-1922 (OPM Production: Apr. 29, 2016).

[622] *Id.*; E-mail from [redacted] to CIRT (OPM) (Apr. 15, 2015, 6:54 p.m.) at HOGR0724-000868 (OPM Production: Dec. 22, 2015).

[623] *See Supra,* Chapter 4: The Role of Cylance.

4. There is no evidence showing CyTech leaked information about their involvement in responding to the OPM breach to the media. In fact, after the *Wall Street Journal* contacted CyTech on June 9, 2015, (the day before the paper reported CyTech discovered the breach), CyTech immediately contacted OPM. CyTech coordinated with OPM Director of IT Security Operations Jeff Wagner on CyTech's response to the reporter, and CyTech's clarification that they did not advise OPM personnel concerning the incident a year ago. Wagner responded to CyTech's proposed response to the *Wall Street Journal* via email. He wrote: "correct away."[624]

5. Testimony from former OPM Chief Information Officer Donna Seymour to the Committee on June 24, 2015 regarding the CyTech matter is inconsistent with documents and testimony from other witnesses.[625] Seymour testified that OPM purchased CyTech licenses. In fact, OPM did not make any purchases from CyTech. Seymour also testified that CyTech's CyFIR appliance was installed in a quarantine environment for the demonstration. In fact, the CyFIR tool, which runs against programs running in live memory, was running on a live environment when it identified malware on April 22, 2015. Seymour testified that CyTech was given some information regarding indicators of compromise prior to installing the CyFIR appliance on the live IT environment for the demonstration. In fact, CyTech was not given information on indicators of compromise until after they discovered malware on April 22, 2015.

CyTech Is a Small Business Contractor with Significant Cyber Tool Capabilities

CyTech is a service disabled veteran-owned small business. The company was started in 2003 by CEO Ben Cotton. Prior to starting CyTech, Cotton served for more than twenty years in Army Special Forces and specialized in computer forensics. Cotton told the Committee that after he retired, he started CyTech to provide "computer forensics, e-discovery collection, sensitive site exploitation support to the U.S. Government, the intel community, and SOCOM [Special Operations Command], as well as commercial entities."[626] Over the course of his career, Cotton has been qualified as an expert witness on computer forensic matters in a number of matters at the federal and local level.[627] CyTech's clients include military and intelligence entities as well as a major commercial manufacturer.[628]

CyTech offers cyber-related services that include a tool referred to as CyTech Forensics and Incident response (CyFIR). The CyFIR tool was released for public sale in 2014.[629] Cotton described CyFIR in his testimony to the Committee. He stated: "fundamental to CyFIR is a concept we call speed to resolution. . . . which is the ability to identify malware or breach

---

[624] Cotton Tr., Ex. 9.
[625] *Hearing on OPM Data Breach: Part II* (statement of Donna Seymour, Chief Info. Officer, Office of Pers. Mgmt.).
[626] Cotton Tr. at 6.
[627] Cotton Tr. at 6-7.
[628] Cotton Tr. at 7.
[629] Cotton Tr. at 8.

conditions inside of a network, to investigate those anomalies, to isolate them, and to remediate them."[630] He also stated:

> The value add to CyFIR is the speed that we can perform these discovery, investigative and remediation functions . . . specifically in the incident response and the network forensics realms. We have the ability to simultaneously conduct searches and do assessments on every single end point inside of an environment. EnCase [a competing tool], due to its technology limitations, can only search a limited subset of that, and the number of . . . end points that it can search is dependent upon basically the network infrastructure and the ability for it to pull that data from the end points back to the investigative console. . . . our search results . . . can come back to us in as little as 45 seconds, where with the other competitive tools, which EnCase is one of them, that typically takes days or weeks to get that information back.[631]

Cotton also stated that CyFIR is "designed to run in a live environment" and it is "not a dead drive forensics tool."[632] He testified about the challenges of modern cyber threats. He stated: "we need to eliminate the time constraints that are imposed by using dead drive forensics tools to investigate incident response. And so we've done that [with CyFIR]. We operate strictly on live systems."[633]

In 2014, CyTech began promoting the CyFIR tool through outreach to various partners and an exhibition at the 2014 RSA Security LLC conference.[634] This outreach ultimately led to the demonstration of the CyFIR tool at OPM on April 21, 2015.

CyTech Was Invited to Conduct a Demo at OPM

In response to the OPM cyber incident first identified in March 2014 and after subsequently identifying serious vulnerabilities in the OPM network, OPM initiated the IT Infrastructure Improvement project.[635] In June 2014, OPM awarded a sole source contract to Imperatis to serve as prime contractor for the project.[636] As part of this contract, the prime contractor was directed to identify, evaluate and recommend security tools to secure OPM's legacy IT environment and design and build a secure new IT environment. CyTech was among the tools that Imperatis and OPM considered as part of this effort.[637]

---

[630] Cotton Tr. at 8.
[631] Cotton Tr. at 9.
[632] Cotton Tr. at 10.
[633] *Id.*
[634] Cotton Tr. at 8; *CyFIR*, RSA CONFERENCE, http://www.rsaconference.com/events/us14/exhibitors-sponsors/exhibitor-list/1139/cyfir (last visited April 10, 2016) (list of products available at 2014 RSA Conference).
[635] *OPM Data Breach: Hearing Before the H. Comm. On Oversight and Gov't Reform*, 114th Cong. (June 16, 2015) (statement of Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt.).
[636] Imperatis Letter Contract (June 16, 2014), Attach. 1 at 000003 (Imperatis Production: Sept. 1, 2015). A sole source contract is a contract that was awarded without being subject to the competitive bidding process. *See Infra,* Chapter 8: The IT Infrastructure Improvement Project: Key Weaknesses in OPM's Contracting Approach.
[637] Security Tool/Vendor Demonstrations, Attach. 11 at 001441-42 (Imperatis Production: Sept. 1, 2015).

Prior to the April 21, 2015 CyFIR Demonstration at OPM

Documents and testimony show OPM had interest in the CyFIR tool beginning in February 2015, and meetings were scheduled to learn more about the tool.[638] Imperatis coordinated two meetings for OPM at CyTech headquarters to discuss the CyFIR tool on March 27, 2015 and April 2, 2015.[639]

At the March 27 meeting, according to Cotton, Wagner's reaction to the CyFIR tool was "very positive" and OPM requested another meeting to include additional OPM staff.[640] At the April 2 meeting, according to Cotton, Wagner's reaction was again "extremely positive" and OPM told CyTech they wanted CyTech to bring the CyFIR appliance to OPM for a demonstration to "let them kick the tires . . . on CyFIR inside their environment."[641]

Wagner testified that "CyTech was a potential replacement of our current EnCase capability, because they were indicating that their client tool was able to take the forensic image remotely and then transmit the image file back instead of a piece of the image file at a time."[642]

After these two meetings, the onsite CyFIR demonstration was scheduled for April 21, 2015 at OPM headquarters.

The April 21, 2015 – April 22, 2015 CyFIR Demonstration at OPM

In preparation for the demonstration at OPM headquarters, CyTech ordered and configured a CyFIR appliance.[643] Then, on April 20, 2015, Imperatis employee [redacted] informed Wagner that the CyFIR tool was ready for the OPM team to "give it a run through" and that Cotton was available to be on site with demo licenses for about fifty agents.[644] On the morning of April 21, 2015, Cotton arrived at OPM headquarters for the demonstration.[645]

---

[638] Email from Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt., to Matthew Morrison, Assurance Data, Inc. (Feb. 23, 2015, 1:51 p.m.), at HOGR020316-000292 (OPM Production: Feb. 16, 2016).

[639] Security Tool/Vendor Demonstrations, Attach. 11 at 001441-42 (Imperatis Production: Sept. 1, 2015); Cotton Tr., Ex. 1; Email from [redacted] Imperatis, to Jonathon Tonda, Contractor, U.S. Office of Pers. Mgmt.(Mar. 30, 2015, 1:51 p.m.), at HOGR020316-000298 (OPM Production: Feb. 16, 2016); Imperatis Weekly Report (Mar. 30, 2015 to Apr. 3, 2015), Attach. 6 at 000704 (Imperatis Production: Sept. 1, 2015).

[640] Cotton Tr. at 12-13; Email from Imperatis to H. Comm. on Oversight & Gov't Reform Majority Staff (Sept. 1, 2015) (stating after the March 27, 2015 meeting "Wagner requested an additional follow up meeting for several members of his staff to be briefed on CyFIR.") (on file with the Committee).

[641] Cotton Tr. at 13; Apr. 2, 2015 Meeting Acceptance by Brendan Saulsbury, Senior Cyber Security Engineer, SRA (Mar. 31, 2015), at HOGR020316-000301 (OPM Production: Feb. 16, 2016); Email from Imperatis to H. Comm. on Oversight & Gov't Reform Majority Staff (Sept. 1, 2015) (stating OPM interested in the CyFIR tool and a subsequent meeting was arranged for an onsite CyFIR demonstration) (on file with the Committee).

[642] Wagner Tr. at 97-98.

[643] Cotton Tr., Ex. 2 (CyFIR Appliance and Configuration Invoice for $7943 (Apr. 3, 2015)).

[644] Email from [redacted] Imperatis to Jeff Wagner, Dir. Info. Tech. Sec. Operations and Jonathan Tonda, Contractor, U.S. Office of Pers. Mgmt. (Apr. 20, 2015, 4:22 p.m.), at HOGR0909-000007 (OPM Production: Oct. 28, 2015).

[645] OPM Visitor Log, Washington, D.C. (Apr. 21, 2015), at HOGR020316-000522 (OPM Production: Feb. 16, 2016). On September 28, 2015, OPM produced a highly redacted version of the above cited visitor log in response to a July 24, 2015 request. The initial version was so heavily redacted that no names were provided, including

Wagner testified that he forgot the demonstration had been scheduled, but he decided to go forward with the demonstration "because we had something interesting going on, it would be interesting to see what the tool could do."[646] The decision to conduct a demonstration in the midst of an incident response effort is interesting given the severity of the incident.

During a demonstration of the CyFIR tool, CyTech usually provides a license with a limited number of agents to be deployed. For purposes of the OPM demonstration that began on April 21, Cotton testified: "we had a very limited license on the number of agents."[647] Cotton stated CyTech arranged for twenty agents to be pushed out by OPM for the demonstration.[648]

Cotton stated that OPM did not give him any specific instructions or configurations prior to the April 21, 2015 demonstration, nor was he given indicators of compromise to look for when the CyFIR appliance was installed.[649] The agency later claimed that indicators of compromise were given to CyTech prior to installation.[650] The documents and testimony show, however, that CyTech was recruited to provide assistance to OPM and given indicators of compromise only after it had successfully identified malware in the live environment.

With respect to where the appliance was installed on April 21, 2015, Cotton testified: "we left it up to OPM as to what computers or what environment we would be put into."[651] In other words, it was up to OPM to decide where to deploy the CyFIR agents.

Cotton stated he spent a significant amount of time waiting for permissions and access to IT facilities on April 21. By the time the CyFIR appliance was installed it was late in the day and Cotton's escort "had to catch a bus" so the demonstration had to continue the next day.[652] Before he left, Cotton activated the CyFIR tool's cyber threat assessment function, which takes a snapshot of all the computers where CyFIR is installed and then compares the snapshot against "known good, known bad, and unknown processes."[653]

There is no evidence that shows CyTech received specific information about where on the OPM network CyFIR was deployed. Documents and testimony do show, however, that on April 21, 2015, the CyFIR tool was deployed to a live production environment where it identified malware when results of the demonstration were examined the following day. Wagner

---

Cotton's. After multiple requests and almost seven months after the initial request, the Committee finally obtained a readable version of the OPM visitor log in February 2016.

[646] Wagner Tr. at 99.

[647] Cotton Tr. at 16.

[648] *Id.*

[649] Cotton Tr. at 14, 16.

[650] Notably, OPM appears to assert that an April 23, 2015 email exchange supports the statement that OPM provided the indicators of compromise to CyTech to find the malware prior to the April 21/22 CyFIR demonstration. *See* Email from Jonathon Tonda, Contractor, U.S. Office of Pers. Mgmt., to Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt. (June 15, 2015, 2:35 p.m.) with Attach. Email from Brendan Saulsbury Senior Cyber Security Engineer, SRA, to [redacted] Imperatis (Apr. 23, 2015, 12:47 p.m.), at HOGR020316-000254 (OPM Production: Feb. 16, 2016).

[651] Cotton Tr. at 16.

[652] *Id.*

[653] Cotton Tr. at 16-17.

testified the tool was deployed in a live production environment and that the CyFIR tool did identify malware.[654]

In fact, OPM's Production Change Request Form for the April 21, 2015 CyFIR demonstration was signed by Wagner that day. It states that the Change Request was "Urgent"; that the "Need/Justification" for deploying CyFIR was because "Security needs to stand up and deploy CyFIR to investigate incident"; and that the "Implementation Plan" was to "Rack, configure and deploy CyFIR products and test in production environment."[655]



9. Need/Justification: Security needs to stand up and deploy CyFir to investigate incident	10. Impact Factor: ☐ 1 (Major) ☐ 2 (Significant) ☐ 3 (Minor) ☒ 4 (Standard)
11. Implementation Plan: Rack, configure and deply CyFir products and test in Production environment	12. Users Affected? No

The Change Request Form lists five areas where the CyFIR tool was to be deployed on April 21, 2015—all five were live production servers. The next day, on April 22, 2015, Cotton returned to OPM to continue the demonstration.[656] Upon arrival, Cotton accessed the CyFIR threat assessment screen and found the tool had identified known malware as well as "a subset of unknown processes . . . masquerading as McAfee executables" according to the CyFIR categorization system.[657]

Cotton testified he put the malware CyFIR found on a thumb-drive and gave it to [redacted] who worked for Imperatis and was escorting Cotton at OPM.[658] Cotton stated that he believed [redacted] provided the information to OPM IT Security Operations. Wagner testified "CyFIR was able to find malware within the [OPM IT] environment" and was deployed in a live environment.[659]

US-CERT confirmed Cotton's assessment that CyFIR found malware on a key server. In fact, four of the five servers that CyFIR was loaded onto April 21, 2015 were implicated in the personnel and background investigation data breach.[660] While CyTech's CEO was not told

---

[654] Wagner Tr. at 102-103. The OPM Director of IT Security Operations added that CyFIR "did not find specifically anything that we hadn't already found." *Id.* at 16.

[655] OPM Production Change Request Form for Apr. 21, 2015 CyFIR Demonstration, at HOGR0909-000090-91 (OPM Production: Oct. 28, 2015).

[656] OPM Visitor Log, Washington, D.C. (Apr. 22, 2015), at HOGR02316-000525 (OPM Production: Feb. 16, 2016).

[657] Cotton Tr. at 19.

[658] *Id.* In February 2016, the Committee inquired with Imperatis, [redacted] employer, about the status of this thumb drive, but the thumb drive was not located. Notably, Imperatis stated Mr. Cotton did not provide a thumb drive to [redacted] with incident response data, but [redacted] was told by another CyTech employee such a thumb drive was given to the FBI. Imperatis Memo to Majority Staff (Feb. 3, 2016), on file with staff.

[659] Wagner Tr. at 102-103. The Director [Wagner] added that "it did not find specifically anything that we hadn't already found." *Id.* at 102.

[660] OPM Production Change Request Form for Apr. 21, 2015 CyFIR Demonstration, at HOGR0909-000090 to 91 (OPM Production: Oct. 28, 2015).

going into the demonstration that all of the malware Cylance identified on April 21, 2015 had been previously identified with the Cylance tools, it is indisputable that CyFIR did identify malware on four of the five servers it was deployed to during the April 21, 2015 product demonstration. The documents show:

- CyFIR was installed on server [redacted] on April 21, 2015.[661] On this server [redacted] which is believed to be a workstation, Cylance found the [redacted] malware on April 21, 2015 and discussed it via email at 12:51 a.m.[662] [redacted] was a [redacted] Hikit that pointed to the malicious domain [redacted] CyFIR identified malware on this server April 21, 2015.[663] This information was provided to US-CERT and it subsequently appeared in US-CERT's May 4, 2015 Preliminary Digital Media Analysis Report.[664]

- CyFIR was installed on server [redacted] on April 21, 2015.[665] On this server [redacted] CylanceProtect also found the Trojan [redacted] on April 21, 2015 and discussed it via email at 12:51 a.m.[666] [redacted] was a Hikit RAT (Remote Administration Tool) and the DLL (Dynamic Link Libraries) would attempt to read a configuration file in the same folder it was executed.[667] CyTech identified malware on this server. This information was provided to US-CERT, and it subsequently appeared in US-CERT's May 4, 2015 Preliminary Digital Media Analysis Report.[668]

- CyFIR was installed on [redacted]—a key Microsoft database server. It was on this server that CylanceV initially identified the malicious executables on April 16, 2015 that US-CERT would affirm as a malicious PlugX package on April 17, 2015.[669] CyTech identified malware on this server.

- CyFIR was installed on server [redacted] on April 21, 2015.[670] CylanceProtect would identify a RAR SFX2 folder on this server that was created in a

---

[661] U.S. Dep't of Homeland Security/US-CERT, Preliminary Digital Media Analysis-INC465355-A (May 4, 2015) at HOGR0724-001032 (OPM Production: Dec. 22, 2015); Briefing by U.S. Office of Pers. Mgmt. to H. Comm. on Oversight & Gov't Reform Staff (Apr. 18, 2016).

[662] Coulter Tr., Ex. 7.

[663] *Id.*

[664] U.S. Dep't of Homeland Security/US-CERT, Preliminary Digital Media Analysis-INC465355-A (May 4, 2015) at HOGR0724-001032 (OPM Production: Dec. 22, 2015); Briefing by U.S. Office of Pers. Mgmt. to H. Comm. on Oversight & Gov't Reform Staff (Apr. 18, 2016).

[665] *Id.*

[666] Coulter Tr., Ex. 7. *See also* Coulter Tr., Ex. 3.

[667] U.S. Dep't of Homeland Security/US-CERT, Malware Analysis Report-460357-A (April 24, 2015) at 000190 (US-CERT Production: Dec. 11, 2015).

[668] U.S. Dep't of Homeland Security/US-CERT, Preliminary Digital Media Analysis-INC465355-A (May 4, 2015) at HOGR0724-001032 (OPM Production: Dec. 22, 2015); Briefing by U.S. Office of Pers. Mgmt. to H. Comm. on Oversight & Gov't Reform Staff (Apr. 18, 2016).

[669] Email from [redacted] to Brendan Saulsbury, Senior Cyber Sec. Engineer, SRA (Apr. 17, 2015, 5:19 p.m.) at HOGR0724-000872- 75 (OPM Production: Dec. 22, 2015).

[670] U.S. Dep't of Homeland Security/US-CERT, Preliminary Digital Media Analysis-465355 (May 4, 2015) (OPM Production: Oct. 28, 2016); Briefing by U.S. Office of Pers. Mgmt. to H. Comm. on Oversight & Gov't Reform Staff (Apr. 18, 2016).

"McAfeeSVC" folder in a directory—a folder that was part of a malicious PlugX package. This RAR SFX2 would also be found on its aforementioned duplicate server [redacted] CyTech identified malware on this server.

- CyFIR was installed on sever [redacted] on April 21, 2015. The documents obtained by the Committee do not make reference to this server.

According to Cotton, around lunchtime on April 22, 2015, there was a brief meeting between Wagner and [redacted] Cotton's escort.). Wagner asked, "they found it?"[671] [redacted] nodded.[672] Cotton testified that Wagner requested "an emergency purchase order for CyFIR inside of the legacy [IT environment]" for a license with 15,000 agents and several CyFIR appliances as well as 1,000 hours for personnel support.[673]

Cotton testified that on April 22, 2015, he offered incident response and forensic assistance to OPM, and OPM accepted.[674] Cotton subsequently met briefly with US-CERT and the FBI to describe CyFIR findings and said it was his understanding that "OPM had turned over the malware that we had imaged that morning to them [US-CERT]."[675] Late on April 22, 2015, Cylance began working with CyTech and requested that CyTech pull system files to support forensic analysis.[676] Cotton testified that he contacted CyTech's senior incident response expert, Juan Bonilla, who was not part of the original demonstration, and directed him "to fly in as early as he could to assist with the incident response."[677]

The documents and testimony show OPM quickly escalated the use of CyFIR within the agency's environment after CyFIR successfully identified malware. For example, on April 22, 2015, at 3:53 p.m., CyFIR was loaded on server [redacted][678] This server provided access to the PIPS mainframe.

On April 23, 2015, CyFIR was loaded on its duplicate server [redacted].[679] CyFIR was put on servers [redacted] and [redacted] on April 17, 2015, and the images CyFIR extracted from these two servers were supplied to US-CERT appeared in US-CERT's May 4, 2015 Preliminary Digital Media Analysis Report.[680] These

---

[671] Cotton Tr. at 20.
[672] *Id.*
[673] *Id.*
[674] Cotton Tr. at 39-41.
[675] Cotton Tr. at 27; CyTech Demonstration/Results Participants, at HOGR0724-000322 (OPM Production: Sept. 25, 2015) (showing CyTech demonstration/ results participants included FBI, US-CERT, OPM, OPM contractors, Imperatis, and Cytech).
[676] Email from Chris Coulter, Managing Dir., Cylance to Ben Cotton, Chief Exec. Officer, CyTech (Apr. 22, 2015, 7:01 p.m.), at HOGR020316-000008 (OPM Production: Feb. 16, 2016).
[677] Cotton Tr. at 25. Cotton noted that CyTech's expert, Bonilla, as a senior member of the CyTech team, is typically billed at between $450 and $350 an hour. *Id.*
[678] U.S. Dep't of Homeland Security/US-CERT, Preliminary Digital Media Analysis-465355 (May 4, 2015) (OPM Production: Oct. 28, 2016); Briefing by U.S. Office of Pers. Mgmt. to H. Comm. on Oversight & Gov't Reform Staff (Apr. 18, 2016).
[679] *Id.*.
[680] *Id.*.

servers [redacted] are also critical because it provided access to the PIPS mainframe.

US-CERT's reports show CyFIR was placed on an additional key server and its duplicate [redacted] on April 23 at 2:27 p.m.[681] This sever is a critical jump box that provided access to the portion of OPM's environment segments where the PIPS mainframe resides.[682] While Cylance was installed on these servers at 6:21 p.m. on April 17, 2015, CyFIR was assisting with forensic work.

Documents show OPM, after reviewing the results of the CyTech demonstration, deployed CyFIR to key servers that gave access to critical parts of OPM's environment, including one of the most important and sensitive servers that gave access to the PIPS mainframe, where sensitive background investigation data was stored. This suggests OPM believed CyTech could assist the agency in the incident response situation.

By April 24, 2015, and in response to Wagner's verbal request for services, CyTech submitted a quote to OPM through Imperatis.[683] CyTech quoted $818,000 for a perpetual license with 15,000 agents.[684] The documents show there was a serious effort to finalize OPM's verbal request for services and that the participants in the April 22 meeting understood OPM's intent. Sometime the week of April 27, Imperatis reported "coordinating equipment installation and configuration with security vendors" including "working to finalize BOM [bill of materials]" for CyFIR.[685] In an interview with the Committee, Wagner testified that he did not say OPM would buy CyFIR, but acknowledged that he likely asked for a quote.[686] CyTech relied on the request for services that exceeded the scope of a typical demonstration and expanded the services it provided to OPM during the 2015 incident response period. Consequently, on April 22, 2015, CyTech provided a license to OPM for 1,000 endpoints that expired on June 30, 2015.[687]

Cotton testified that CyTech provided incident response and forensic assistance to OPM out of a sense of duty and with the expectation that there would be a contractual arrangement put into place.[688] Cotton stated there was a promise of a contract, but execution was delayed repeatedly.[689] With respect to why CyTech provided these services without a contract in place, Cotton testified:

---

[681] U.S. Dep't of Homeland Security/US-CERT, Preliminary Digital Media Analysis-465355 (May 4, 2015) (OPM Production: Oct. 28, 2016); Briefing by U.S. Office of Pers. Mgmt. to H. Comm. on Oversight & Gov't Reform Staff (Apr. 18, 2016).
[682] Saulsbury Tr. At 75-76.
[683] Cotton Tr., Ex. 3,4 (CyTech Price Quote ($818,000) for Emergency Purchase Order (Apr. 24, 2015) and CyTech Transmittal email to Imperatis for CyTech Quote (Apr. 24, 2015)).
[684] *Id.*
[685] Imperatis Weekly Report (Apr. 27, 2015-May 1, 2015), Attach 6 at 000758 (Imperatis Production: Sept. 1, 2015).
[686] Wagner Tr. at 104.
[687] Cotton Tr. at 25; *see also* Email from Ben Cotton, Chief Exec. Officer, CyTech, to H. Comm. on Oversight & Gov't Reform Majority Staff (Apr. 16, 2016) (confirming the nature of the licensing arrangement as of April 22, 2015) (on file with the Committee).
[688] Cotton Tr. at 41.
[689] Cotton Tr. at 40.

> Typically, there is [a contract in place]. It's also atypical that we are doing a demonstration and we find live malware on the end points of a government agency that, quite frankly, controls my security clearance. I knew immediately, once it was determined that this was malware, what the implications could be for the country. So, you know, maybe I'm a bad businessman, maybe I'm too much of a patriot at this point, but I didn't want to leave them in the lurch and I didn't want to let this breach go without a capability that would help minimize this to OPM.[690]

Just days before OPM denied CyTech's role in the response to the media, OPM personnel and Imperatis shared internally the clear expectation that OPM would be compensating CyTech for CyFIR and incident response and forensic support based on the conversations CyTech had with OPM in mid-April 2015. On June 5, 2015, Imperatis inquired about the status of the CyTech quote. An Imperatis employee asked an OPM official: "do you want CyFIR for the existing network, I assume yes to compliment your Encase tool?"[691]

Message

From: Patrick Mulvaney [redacted]
Sent: 6/5/2015 8:45:01 PM
To: Wagner, Jeffrey P. [redacted] XCHANGE ADMINISTRATIVE GROUP
([redacted] RECIPIENTS/[redacted] IPWagner]; Tonda, Jonathan D.
[redacted]
CC: [redacted]
Subject: CyFir

Jeff/Jon,

I know you are in the thick of it right now. Wanted to get some clarification and direction with regards to forensics and CyFir.

Had a conversation with the Cytech team today who were following up on a few items, I told them for Shell we had some time before we were procuring forensics. You may have a higher immediate need for it that would trump our timeline. Can you answer some of these below;

1. The status of the loaner appliance – Do you want them to pick up the appliance or is it currently supporting an active investigation? Do you want to possibly leave it in place assuming an upcoming procurement with CyFir? I was under the impression the licenses for it have expired.
2. Do you want CyFir for the existing network, I assume yes to compliment your Encase tool? If so how quickly do you need it and do you foresee that being procured off our contract or yours and scoped to support both sides?
3. I can't recall with the current BOM, where the 6 appliances were destined for, somehow we got to that number but I don't recall the justification, HA config, or physical location for them. I need to be sure there is enough for Shell and Existing.

Thanks,

Patrick Mulvaney

atment Requested For Committee and Staff Use Only

[690] Cotton Tr. at 40-41.

[691] Email from Patrick Mulvaney, Imperatis to Jeff Wagner, Dir. Info. Tech. Security Operations, U.S. Office of Pers. Mgmt. (June 5, 2015, 8:45 p.m.), at HOGR0909-000046 (OPM Production: Oct. 28, 2015).

The CyTech Demo Turned into Incident Response and Forensic Support

In mid-April through May 2015, significant incident response and forensic support activity was underway at OPM. Documents and testimony show CyTech was part of that effort. Other contractors that were onsite confirmed CyTech's role. Cylance was one such contractor. A Cylance official testified CyTech was providing assistance onsite with a tool "that can make it easier to obtain evidence" and that "having that [tool] actually was useful. It sped up the initial triage process of trying to obtain critical forensic artifacts."[692]

Another contractor who staffed the OPM IT Security Operations group said, "…OPM made a decision to have the CyFIR product…assist with gathering forensic images, of some of the servers, that US-CERT requested the image."[693] Yet another OPM contractor, Imperatis, reported that "CyFIR (forensics tool) [was] installed in legacy environment through operational testing" and "has proven to be extremely beneficial in the reduction of man hours required with an active security issue."[694]

CyTech Provided Onsite Incident Response and Forensic Support From April 23 to May 1, 2015

The Committee obtained documents and testimony that show CyTech provided specific incident response and forensic support activities to OPM. On April 23, 2015, after the CyFIR demonstration, Cotton returned to OPM to provide assistance.[695] Cotton also brought a CyTech expert, Juan Bonilla, whose services are billed at $350 to $450 an hour, to assist OPM with the CyFIR tool.[696] Bonilla remained onsite at OPM through May 1, 2015.[697] Documents show that it was an incident response and forensic support environment at that time. The FBI and US-CERT were also onsite on April 23, 2015 and returned for several days thereafter.[698]

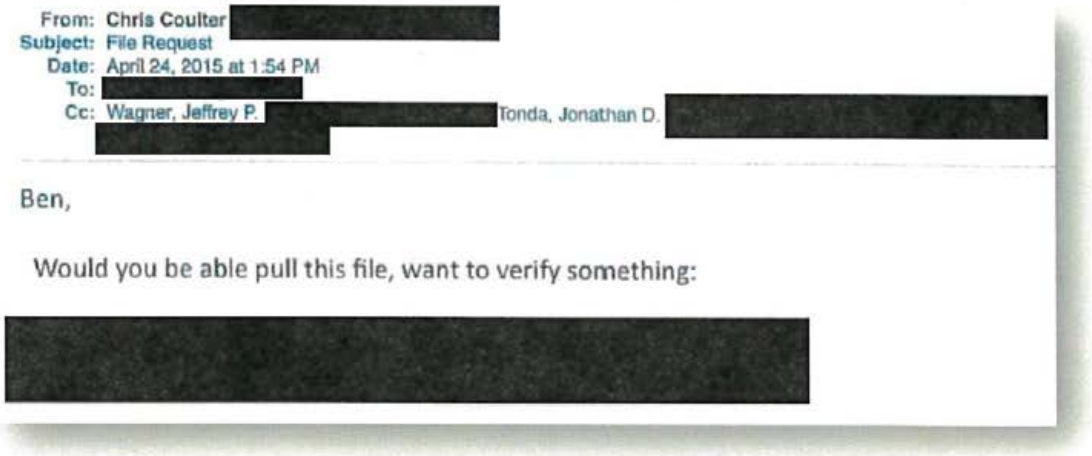
In testimony to the Committee and in public statements, OPM officials downplayed CyTech's role in the incident response and forensic support operation in April-May 2015. For example, Wagner testified Bonilla "wasn't really part of the investigation."[699] In an email from April 28, 2015, however, Wagner notified OPM IT administrators that Bonilla would be

---

[692] Coulter Tr. at 68-69.
[693] Saulsbury Tr. at 84.
[694] Imperatis Weekly Report (Apr. 20, 2015-Apr. 24, 2015), Attach. 6 at 000743 (Imperatis Production: Sept. 1, 2015).
[695] OPM Visitor Log Washington, D.C. (Apr. 23, 2015) at HOGR020316-000530 (OPM Production: Feb. 16, 2016).
[696] *Id.*; Cotton Tr. at 25.
[697] Cotton Tr. at 26; Email from Juan Bonilla, Senior Sec. Consultant, CyTech, to Jonathan Tonda, Contractor and Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt. (May 1, 2015, 12:43 p.m.), at HOGR020316-000067 (OPM Production: Feb. 16, 2016) (showing Bonilla coordinating collection of images with OPM prior to May 1 departure); Email from Juan Bonilla, Senior Sec. Consultant, CyTech, to Jonathan Tonda, Contractor, U.S. Office of Pers. Mgmt. (May 1, 2015, 5:09 p.m.), at HOGR020316-000068 (OPM Production: Feb. 16, 2016) (indicating Bonilla left CyFIR credentials for OPM's use).
[698] OPM Visitor Log, Washington, D.C. (Apr. 23, 2015), at HOGR020316-000529-30 (OPM Production: Feb. 16, 2016).
[699] Wagner Tr. at 101.

"assisting with an investigation over the next two weeks" and asked what needed to be done to obtain system access for him.[700] Wagner also testified Bonilla and Coulter worked together during the incident response. Wagner stated: "we threw everybody into a giant room, and Juan [Bonilla] was the CyTech engineer, much like Coulter was the Cylance engineer. . . ."[701] Clearly, Cylance had a significant role in incident response and the comparison between CyTech and Cylance personnel onsite suggests at the very least CyTech played a supporting role in incident response that OPM has not publicly acknowledged.

In terms of other specific CyTech activities, Cotton testified CyTech was initially asked to image all the random access memory from approximately fifty computers, image the hard drives for those computers, and pull event logs for OPM.[702] CyTech also worked with Cylance to fulfill their requests for files. For example, on April 24, 2015, Cylance asked CyTech to pull a ".bat" file.[703] Cotton testified that ".bat" files "are commonly used as part of a breach to automate the infestation or the installation of malware."[704]


From: Chris Coulter [redacted]
Subject: File Request
Date: April 24, 2015 at 1:54 PM
To: [redacted]
Cc: Wagner, Jeffrey P. [redacted] Tonda, Jonathan D. [redacted]

Ben,

Would you be able pull this file, want to verify something:

[redacted]

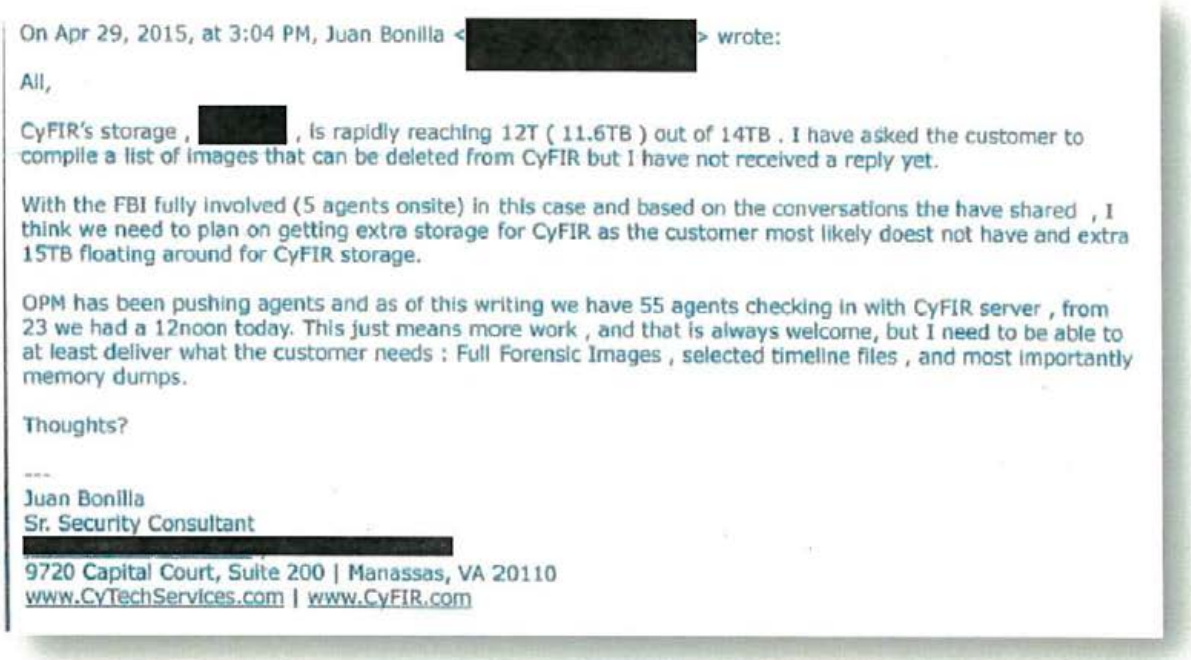
Bonilla worked with OPM to deploy CyFIR and coordinated with OPM staff to address connectivity issues.[705] Documents show that as of April 28, 2015, Wagner prioritized CyFIR deployment to at least thirty-eight servers.[706]

Documents show CyTech collected thousands of images in its forensic support role. Indeed, the documents show the CyFIR appliance was literally running out of memory space to retain all of these images. On April 29, 2015, Bonilla requested information from OPM about a

---

[700] Email from Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt., toJames Anderson, U.S. Office of Pers. Mgmt. (Apr. 28, 2015, 5:43 p.m.) at HOGR020316-000707 (OPM Production: Mar. 16, 2016).
[701] Wagner Tr. at 100.
[702] Cotton Tr. at 27-28.
[703] Email from Chris Coulter, Managing Dir., Cylance to Ben Cotton, Chief Exec. Officer, CyTech (Apr. 24, 2015, 5:54 p.m.) at HOGR020316-000010 (OPM Production: Feb. 16, 2016).
[704] Cotton Tr. at 29.
[705] Emails between Juan Bonilla, Senior Sec. Consultant, CyTech, and Brendan Saulsbury, Senior Cyber Security Engineer, SRA (Apr. 27, 2015) at HOGR020316-000026-28 (OPM Production: Feb. 16, 2016).
[706] Message from [redacted] Contractor, U.S. Office of Pers. Mgmt., to Jonathan Tonda, Contractor, U.S. Office of Pers. Mgmt. (Apr. 28, 2015, 9:04 p.m.) at HOGR020316-000333 (OPM Production: Feb. 16, 2016).

list of images that needed to be retained because the CyFIR appliance only had fourteen terabytes of storage space and was quickly nearing capacity.[707] Cotton testified that OPM asked CyTech "to collect all this information and we were running out of storage for that."[708]



On Apr 29, 2015, at 3:04 PM, Juan Bonilla <[redacted]> wrote:

All,

CyFIR's storage , [redacted] , is rapidly reaching 12T (11.6TB) out of 14TB . I have asked the customer to compile a list of images that can be deleted from CyFIR but I have not received a reply yet.

With the FBI fully involved (5 agents onsite) in this case and based on the conversations the have shared , I think we need to plan on getting extra storage for CyFIR as the customer most likely doest not have and extra 15TB floating around for CyFIR storage.

OPM has been pushing agents and as of this writing we have 55 agents checking in with CyFIR server , from 23 we had a 12noon today. This just means more work , and that is always welcome, but I need to be able to at least deliver what the customer needs : Full Forensic Images , selected timeline files , and most importantly memory dumps.

Thoughts?

Juan Bonilla
Sr. Security Consultant
[redacted]
9720 Capital Court, Suite 200 | Manassas, VA 20110
www.CyTechServices.com | www.CyFIR.com

It is worth noting, during what would turned out to be most damaging data breach in the history of the federal government, OPM was making decisions about what forensic evidence to retain without it appears consulting the OIG or counsel in a meaningful way.

In late April 2015, CyTech and Cylance continued to assist OPM. On April 29, 2015, Cylance and CyTech updated OPM on the status of Cylance's analysis efforts. Coulter testified that there were three teams working on incident response with OPM: Cylance, CyFIR, and law enforcement. With respect to CyTech's role, Coulter stated "as Cylance through CylanceProtect was identifying new instances of malware that were related, we would then request CyFIR to install an agent on that machine to then collect the data for further analysis."[709] An April 29, 2015 email from Coulter stated that CyFIR would install "agents on the scoped hosts and collect data for the other team" and suggested a "formal meeting with the CyFIR & other team members to close out."[710]

---

[707] Email from Juan Bonilla, Senior Sec. Consultant, CyTech, to Brendan Saulsbury, Senior Cyber Security Engineer, SRA (Apr. 29, 2015, 5:26 p.m.) at HOGR020316-000043 (OPM Production: Feb. 16, 2016).
[708] Cotton Tr. at 31; Cotton Ex. 6 (showing internal CyTech discussion about storage options and how such costs may be covered under a contract); Text Message from Jeffrey Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt. to Jonathan Tonda, Contractor, U.S. Office of Pers. Mgmt. (Apr. 30, 2015) at HOGR020316-000347(OPM Production: Feb. 16, 2016) (showing internal OPM discussion on options for CyFIR to dump images).
[709] Coulter Tr. at 71.
[710] Email from Chris Coulter, Managing Dir., Cylance, to Jonathan Tonda, Contractor, U.S. Office of Pers. Mgmt. and Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt. (Apr. 29, 2015, 4:40 p.m.) at HOGR020316-000337 (OPM Production: Feb. 16, 2016).

In sum, CyTech was onsite at OPM from April 21 to May 1, 2015. During that time, CyTech identified malware and provided incident response and forensic support to OPM that exceeded the scope of the product demonstration that began on April 21.

CyFIR Was Deployed on the OPM Network beginning in April 2015 and Remained on OPM's Network through August 2015

Wagner testified that "once Bonilla left the site, we never utilized CyTech's product again."[711] Documents suggest otherwise. After Bonilla left OPM on May 1, 2015, CyTech continued to provide assistance on an as needed basis. On May 8, 2015, Bonilla emailed Wagner to follow up on the work he did the week before and offered to provide additional assistance with the CyFIR tool.[712]

The documents show OPM continued to use the CyFIR tool from May 2015 through early June. For example, on May 7, 2015, Cylance requested CyFIR be deployed to a particular OPM host.[713] On May 28, 2015, an OPM contractor stated that CyFIR had collected images from a key production server.[714] On June 1, 2015, an OPM contractor wrote: "all other security agents are currently running, Cylan[c]e, CyFIR, Forescout."[715]

Documents show the forensic capabilities of the CyFIR tool were a continuing topic of discussion. For example, Imperatis, the OPM contractor who introduced CyTech to OPM, described a May 15, 2015 "forensics capabilities meeting with CyFIR."[716] Documents show there were continuing interactions with CyTech and use of the CyFIR tool through June 2015.[717]

Wagner minimized the scope of the CyFIR deployment in his testimony to the Committee. He stated: "we only deployed their CyFIR client to a select number of machines."[718] Documents show, however, CyFIR's deployment was fairly extensive. The Committee obtained documents that show the CyFIR tool was tested on more than sixty different servers, including key servers connected to the personnel records and background investigation data that was exfiltrated.[719]

---

[711] Wagner Tr. at 105.
[712] Email from Juan Bonilla, Senior Sec. Consultant, CyTech to Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt. (May 8, 2015, 5:49 p.m.) at HOGR020316-000071 (OPM Production: Feb. 16, 2016).
[713] Email from Chris Coulter, Managing Dir., Cylance, to Jonathan Tonda, Contractor, U.S. Office of Pers. Mgmt. (May 7, 2015, 3:56 p.m.) at HOGRO020316-000351 (OPM Production: Feb. 16, 2016).
[714] Email from Jonathan Tonda, Contractor, U.S. Office of Pers. Mgmt., to Brendan Saulsbury, Senior Cyber Security Engineer, SRA (May 28, 2015, 1:43 p.m.) at HOGR020316-000360 (OPM Production: Feb. 16, 2015).
[715] Email from [redacted] Contractor, U.S. Office of Pers. Mgmt. to U.S. Office of Pers. Mgmt. Employees [redacted] (June 1, 2015, 3:28 p.m.) at HOGR020316-000363 (OPM Production: Feb. 16, 2016).
[716] Imperatis Weekly Report (May 18, 2015-May 22, 2015), Attach.6. at 000797 (Imperatis Production: Sept. 1, 2015).
[717] Email from [redacted] U.S. Office of Pers. Mgmt., to Jonathan Tonda, Contractor, U.S. Off. of Pers. Mgmt. (June 2, 2015, 12:00 p.m.) at HOGR020316-000379 (OPM Production: Feb. 16, 2016).
[718] Wagner Tr. at 151.
[719] List of locations on which CyTech's CyFIR was tested at HOGR0724-000320- 321-UR (OPM Production Sept. 25, 2015). Initially, this document was provided with redactions that did not allow a cross reference with key

Documents show the CyFIR tool was deployed on the OPM system through June 2015, and that it was not fully uninstalled until August 2015. On June 25, 2015, an OPM IT official contacted Bonilla for instructions on how "to uninstall the Cyfir software . . . installed a month ago" from a list of more than forty servers, including several servers involved in the background investigation data breach.[720] This request for instructions to uninstall CyFIR occurred the day after former CIO Donna Seymour and Director Katherine Archuleta testified before the Committee about CyTech's involvement in the discovery of the data breach. Seymour and Archuleta testified that CyTech was not involved in the discovery of the data breach; and they did not disclose the involvement of Cylance, who, like CyTech, also did not have a contract in place when OPM's leadership was testifying before the Committee.[721]

Begin forwarded message:

From: '[redacted]
Subject: Uninstall Cyfir
Date: June 25, 2015 at 1:12:24 PM EDT
To: [redacted]
Cc: [redacted]

Juan,

I am trying to uninstall the Cyfir software I installed a month ago for the following servers. Is there a special process to remove them? I don't see the Cyfir software listed in the add and remove program feature.

Please let me know.

Thanks

Server list:

[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted] – Cant ping / rdp
[redacted]
[redacted]
[redacted]
[redacted]

servers involved in the breach with where the CyFIR tool was deployed. In response to the Committee's February 3, 2016 subpoena OPM provided an unredacted version of this list on April 15, 2016.

[720] Email from [redacted], Contractor, U.S. Office of Pers. Mgmt., to Juan Bonilla, Senior Sec. Consultant, CyTech (June 25, 2015); Cotton Tr., Ex. 6; Wagner Tr. at 32-33.

[721] *Hearing on OPM Data Breach: Part II* (statement of Donna Seymour, Chief Information Officer, Office of Personnel Management) (statement of Katherine Archuleta, Dir., U.S. Office of Pers. Mgmt.).

[redacted]
[redacted] – cant ping / rdp
[redacted]
[redacted] – think this is a work station
[redacted]
[redacted] – Cant ping / rdp
[redacted]

[redacted]
Systems Administrator
U.S. Office of Personnel Management
Network Management – Server Operations
1900 E Street, NW | Washington, DC 20415
Phone: 2[redacted] | email [redacted]
SRA International Inc.

Documents show OPM did not finish uninstalling CyFIR until August 2015. The Committee obtained internal agency emails that state the uninstall effort began on June 26, 2015

and was partially complete by June 29, 2015.[722] As of August 18, 2015, OPM determined that as many as twenty-four devices were still "communicating with the CyFIR server."[723]

The documents show CyTech provided significant incident response and forensic support from April 23 through May 1, 2015. CyTech continued to provide services as needed after CyTech personnel were no longer on site at OPM. Further, OPM deployed the CyFIR tool beginning in April 2015 and did not fully uninstall it until August 2015.[724] The documents also show the CyFIR tool was still installed and communicating with the CyFIR server as late as August 2015. CyTech relied on OPM's request for assistance on April 22, 2015 and provided incident response and forensic support services. Then CyTech became the unwilling focus of media attention.

The *Wall Street Journal* Reports on CyTech's Role in the OPM Incident on June 10, 2015

Pieces of the CyTech story became public when the *Wall Street Journal* published a story under the headline "U.S. Spy Agencies Join Probe of Personnel-Records Theft" on June 10, 2015.[725] The story stated:

> Last week, the Office of Personnel Management disclosed that hackers had breached its networks, warning that the personnel records of roughly four million people—many of them current or former government workers—could have been stolen. At the time, OPM said the breach was discovered as the agency 'has undertaken an aggressive effort to update its cybersecurity posture, adding numerous tools and capabilities to its networks.'
>
> But 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.
>
> An OPM spokesman didn't respond to a request for comment.[726]

---

[722] Email from Administrator, U.S. Office of Pers. Mgmt., to Jonathan Tonda, Contractor, U.S. Office of Pers. Mgmt. (Aug. 19, 2015, 11:34 a.m.) at HOGR0909-000160 (OPM Production: Oct. 28, 2015).

[723] Email from Administrator, U.S. Office of Pers. Mgmt., to Brendan Saulsbury Senior Cyber Security Engineer, SRA, and Jonathan Tonday, Contractor, U.S. Office of Pers. Mgmt. (Aug. 18, 2015, 11:32 a.m.) at HOGR0909-000125 (OPM Production: Oct. 28, 2015).

[724] Cotton Tr. at 61.

[725] Damian Paletta & Siobhan Hughes, *U.S. Spy Agencies Join Probe of Personnel-Records Theft*, WALL STREET JOURNAL, June 10, 2015, available at: http://www.wsj.com/articles/u-s-spy-agencies-join-probe-of-personnel-records-theft-1433936969.

The Committee obtained communications between OPM and CyTech related to the media inquiry. The documents show that before the article was published, CyTech coordinated with OPM. There is no evidence to suggest CyTech was the source of the story. Cotton testified:

> We did not intend to find ourselves in the middle of these hearings. And I am just very concerned about the representations that may or may not have been made around this Hill that have actually been relayed to me that OPM is maligning my company's reputation and our capabilities.[727]

CyTech Coordinated with OPM Prior to the June 10, 2015 Story

On June 9, 2015, Cotton received a call from a reporter regarding CyTech's role in the discovering the OPM data breach.[728] The reporter told Cotton he had four sources saying that CyTech discovered the OPM breach and that CyTech had been advising OPM about this matter for the last year.[729] The reporter requested a comment.[730] Cotton said the reporter could email him about the story, but that he would not comment.[731] Cotton wanted something in writing to confirm the identity of the person on the call.[732]

Late on June 9, 2015, Cotton reviewed the email from the reporter and immediately forwarded it to Wagner for guidance.[733] Cotton asked whether he wanted CyTech to make corrections.[734] Wagner said, "Correct away. Just give me a heads up as to the response so we can discuss."[735]

Cotton proposed a response to the reporter: "[I]t is CyTech policy to not discuss clients or operational matters with the press. CyTech can categorically deny that personnel from CyTech advised OPM personnel concerning this matter a year ago . . . ."[736] Wagner responded early the next day and suggested what amounted to a "no comment" response. Wagner wrote: "[if you] need anything feel free to fire back. Keep the faith."[737]

---

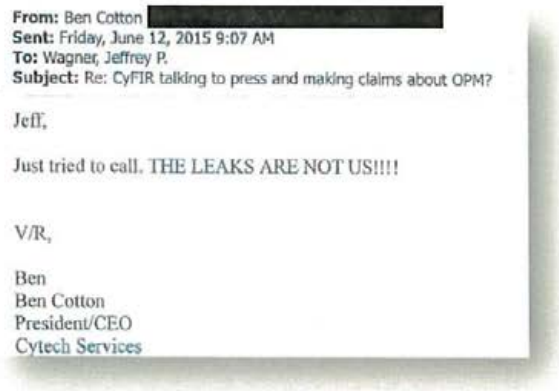
[726] Damian Paletta & Siobhan Hughes, *U.S. Spy Agencies Join Probe of Personnel-Records Theft*, WALL STREET JOURNAL, June 10, 2015, http://www.wsj.com/articles/u-s-spy-agencies-join-probe-of-personnel-records-theft-1433936969.
[727] Cotton Tr. at 107.
[728] Cotton Tr. at 64
[729] *Id.*
[730] *Id.*
[731] *Id.*
[732] *Id.*
[733] Cotton Tr. at 64-65.
[734] Cotton Tr., Ex. 9 (Email from Ben Cotton, Chief Exec. Officer, CyTech, to Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt. (June 9, 2015)).
[735] *Id.*
[736] *Id.*
[737] Email from Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt., to Ben Cotton, Chief Exec. Officer, CyTech (June 10, 2015, 7:14 a.m.) at 2.4 (CyTech Production: Aug. 19, 2015).

OPM and CyTech Respond to the Article

On June 10, 2015, the story was published. It stated: "[F]our people familiar with the investigation said the [OPM] breach was actually discovered during a mid-April sales demonstration at OPM by a Virginia company called CyTech Services, which has a network forensics platform called CyFIR."[738] Wagner testified that this portion of the story was not "accurate in any way."[739]

The story further stated: "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."[740] Coulter, the Cylance engineer onsite at the time of the CyTech demonstration,[741] testified with respect to that portion of the story: "that's actually accurate. They did. They ran a diagnostic study. They may have discovered malware that was embedded on the network, but it was likely already known at that point."[742]

On June 12, 2015, Wagner emailed CyTech about the story. Wagner wrote: "I cannot express how bad this is going down for you. We should talk about this. Call my cell."[743] Cotton quickly responded: "just tried to call. THE LEAKS ARE NOT US!!!" (*emphasis in the original*).[744] In response, Wagner suggested a call with OPM's public affairs office to "work out something that will benefit both organizations."[745] Cotton agreed to discuss the situation.[746]



From: Ben Cotton [redacted]
Sent: Friday, June 12, 2015 9:07 AM
To: Wagner, Jeffrey P.
Subject: Re: CyFIR talking to press and making claims about OPM?

Jeff,

Just tried to call. THE LEAKS ARE NOT US!!!!

V/R,

Ben
Ben Cotton
President/CEO
Cytech Services

---

[738] Damian Paletta & Siobhan Hughes, *U.S. Spy Agencies Join Probe of Personnel-Records Theft*, WALL STREET JOURNAL, June 10, 2015, available at: http://www.wsj.com/articles/u-s-spy-agencies-join-probe-of-personnel-records-theft-1433936969.
[739] Wagner Tr. at 156.
[740] Damian Paletta & Siobhan Hughes, *U.S. Spy Agencies Join Probe of Personnel-Records Theft*, WALL STREET JOURNAL, June 10, 2015, http://www.wsj.com/articles/u-s-spy-agencies-join-probe-of-personnel-records-theft-1433936969.
[741] OPM Visitor Logs, Washington, D.C. (April 21, 22, 2016) at HOGR020316-000521, 524 (OPM Production: Feb. 16, 2016).
[742] Coulter Tr. at 61, Ex. 9.
[743] Cotton Tr., Ex. 10 (Email from Ben Cotton, Chief Exec. Officer, CyTech, to Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt. (June 12, 2015)).
[744] *Id.*
[745] *Id.*
[746] Cotton Tr. at 66, Ex. 10.

In describing OPM's phone conversations with CyTech to the Committee, Wagner testified he had two calls with Cotton on or about June 12, during which the CyTech CEO "acted shocked, assured me it was not him or his company" who had leaked the story.[747] Cotton testified he was surprised by OPM's reaction on the first call and learned OPM was concerned about the story because "the account in the *Wall Street Journal* was inconsistent as to how OPM leadership had already testified to Congress."[748]

Wagner testified that during the second call with OPM's public affairs staff, Cotton again said CyTech was not the source of the story, but he believed Cotton was telling the *Wall Street Journal* that CyTech did in fact have some role in the discovery of the breach.[749]

Cotton, on the other hand, testified that OPM wanted CyTech to sign on to a joint statement that "in essence, it was that *Wall Street Journal* was totally without basis, without fact, and was a lie."[750] Cotton also testified he requested a written draft of OPM's suggested statement, but OPM declined and ultimately CyTech did not agree to their approach because it was "not what actually occurred."[751]

Cotton testified that he explained the whole situation to OPM's public affairs staff, including the April 21, 2015 product demonstration and CyTech's role in incident response and forensic support.[752] Cotton testified that OPM's press spokesman seemed surprised and said he would be in touch, but CyTech did not hear from OPM again.[753] After multiple press inquiries following the story, CyTech issued a press release on June 15, 2015. The press release stated:

> It is CyTech's policy not to discuss our clients or their sensitive operations. However, due to extensive media reporting, we wanted to clarify CyTech's involvement and the assistance we provided in relation to OPM's breach response in April 2015. . . CyTech was initially invited to OPM to demonstrate CyFIR Enterprise on April 21, 2015. . . Using our endpoint vulnerability assessment methodology, CyFIR quickly identified a set of unknown processes running on a limited set of endpoints. This information was immediately provided to the OPM security staff and was ultimately revealed to be malware. CyTech is unaware if the OPM security staff had previously identified these processes. CyTech Services remained on site to assist with the breach response, provided immediate assistance, and performed incident response supporting OPM until May 1, 2015.[754]

---

[747] Wagner Tr. at 153.
[748] Cotton Tr. at 66.
[749] Wagner Tr. at 154.
[750] Cotton Tr. at 68.
[751] *Id.*
[752] *Id.*
[753] Cotton Tr. at 68-69.
[754] Cotton Tr., Ex. 14 (CyTech, Press Release, *CyTech Services Confirms Assistance to OPM Breach Response* (June 15, 2015)). CyTech did produce a draft press release dated June 10, 2015 to the Committee that the CyTech CEO quickly identified as a draft document when questioned about it. This draft press release did not precisely describe CyTech's involvement. The CyTech CEO explained that he revised this draft to the version released June 15 since this was a "public statement against a very large and very powerful government organization, I needed to

The *Wall Street Journal* covered CyTech's public statement in a follow up article on June 15, 2015.[755] In the story, an OPM official stated: "the assertion that Cytech was somehow responsible for the discovery of the intrusion into OPM's network during a product demonstration is inaccurate."[756]

Cotton testified that when he heard OPM's statement, he was concerned because the dispute was starting "to impact our corporate reputation and our capabilities," and he speculated that OPM was parsing words by using the term "discovery of the breach."[757] Cotton testified that "the challenge we had here was clearly you don't want to get into a fight with in the news with one of your clients. But at the same time, to say we had no part in the discovery was clearly false . . . ."[758] Cotton testified that "discovery of the breach" is not precisely defined, and that in his mind, CyTech had "discovered" malware on the system.[759] Cotton stated it was possible "that had somebody noticed a packet going out to an unknown Web site that they could then say, well, we discovered that, because we saw this packet."[760]

The documents show the statement issued by CyTech on June 15, 2015 is consistent with the facts. The documents show CyTech did play a role in identifying malware in the live OPM IT environment and providing incident response and forensic support to OPM beginning in mid-April 2015. The documents show CyTech did not publicly claim to have discovered the intrusion, but rather that it played a role in identifying malware. The agency's strong reaction to the June 10, 2015 story in the *Wall Street Journal* was based on a concern that it contradicted statements senior officials made to Congress about the data breach.[761]

It is troubling that CyTech appears to have in good faith worked to coordinate with OPM on responses to the press while OPM worked to "**kill this cytech crap.**"[762] OPM press officials also demanded that the WSJ print a retraction of the CyTech story on June 10, the day the story

---

be very precise about what my company did and what we didn't do to avoid any entanglements with definitions over "breach discovery." Cotton Tr. at 84-85.

[755] Damian Paletta, *Cybersecurity Firm Says It Found Spyware on Government Network in April*, WALL ST. J., June 15, 2015, available at: http://www.wsj.com/articles/firm-tells-of-spyware-discovery-in-government-computers-1434369994.

[756] *Id.*

[757] Cotton Tr. at 70.

[758] *Id.*

[759] Cotton Tr. at 71.

[760] *Id.*

[761] Cotton Tr. at 66.

[762] Email from Sam Schumach, Press Sec., U.S. Off. of Pers. Mgmt. to Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt. and Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt. (June 18, 2015, 1:25 p.m.) at HOGR020316-000261 (OPM Production: Feb. 16, 2016). OPM appears to have become frustrated with the CyTech story. In a June 23, 2015 email, the OPM Dir. of Communications was coordinating a response to the WSJ on a cybersecurity issue and said to Mr. Wagner, "do you have time to get on the phone with [the reporter] for 10 minutes. I want to make sure he's not trying to resurrect the CyTech Dracula here, in a subtle way." Email from Jackie Koszczuk, Dir. of Comm., U.S. Office of Pers. Mgmt., to Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt. (June 23, 2015, 10:07 p.m.) at HOGR020316-000288 (OPM Production: Feb. 16, 2016).

was published without apparently verifying all the facts surrounding the story and CyTech's role in incident response and forensic support.[763]

OPM Description of CyTech's Role Was Misleading

Testimony and public statements by OPM officials regarding CyTech's role in the data breach incident response and forensic support activities from April to May 2015 were confusing and misleading. OPM was also slow to respond to document production requests regarding this issue further compounding the confusion. When OPM produced documents in early 2016 and as the investigation proceeded, the CyTech narrative became clear. However, when the CyTech story was first reported in June 2015, the details were less than clear and further confused by senior OPM officials' testimony. In June 2015, the CyTech story was the subject of various press reports, including the June 10, 2015 story in the *Wall Street Journal*. On June 16, 2015, former OPM Director Katherine Archuleta testified before the Committee that "OPM detected the intrusion" and denied that contractors did so.[764] Archuleta omitted the fact that Cylance and CyTech played critical roles in identifying the actual malware and providing forensic support.

Archuleta and Seymour Provided Misleading Testimony to Committee

On June 23, 2015, the House Permanent Select Committee on Intelligence (HPSCI) referred evidence to the Committee obtained from CyTech.[765] In light of the press developments and the information from HPSCI, Rep. Turner questioned Seymour and Archuleta about CyTech when they appeared before the Committee on June 24, 2015.[766]



Rep. Mike Turner (R-OH) questions Archuleta and Seymour at June 23, 2015 Committee hearing

[763] Email Jackie Koszczuk, Dir. of Comm., U.S. Office of Pers. Mgmt., to Damian Paletta, Reporter, Wall St. J. (June 10, 2015, 7:15 p.m.) at HOGR020316-000159 (OPM Production: Feb. 16, 2016). The WSJ declined to print a retraction "solely on the basis of the agency's assertion that it is inaccurate." Email from Robert Ourlian, News Editor, Wall St. J., to Jackie Koszczuk, Dir. of Comm., U.S. Office of Pers. Mgmt. (June 10, 2015, 9:26 p.m.) at HOGR020316-00163 (OPM Production: Feb. 16, 2016).

[764] *OPM Data Breach: Hearing Before the H. Comm. on Oversight & Gov't Reform*, 114th Cong. (June 16, 2015) (statement of Katherine Archuleta, Dir., U.S. Office of Pers. Mgmt.).

[765] The House Permanent Select Committee on Intelligence also referred information related to the CyTech matter to the Committee. Letter from the Hon. Devin Nunes, Chairman and the Hon. Adam Schiff, Ranking Member, H. Perm. Select Comm. on Intelligence to the Hon. Jason Chaffetz, Chairman and the Hon. Elijah E. Cummings, Ranking Member, H. Comm. on Oversight & Gov't Reform (June 23, 2015).

[766] *Hearing on OPM Data Breach: Part II.*

Rep. Turner asked Archuleta and Seymour: "was CyTech involved in the discovery of this data breach?" Both witnesses responded no, CyTech was not involved.[767] Documents and testimony do show OPM identified and reported to US-CERT on April 15, 2015 that an unknown Secure Sockets Layer (SSL) certificate was beaconing to a site (opmsecurity.org) not associated with OPM.[768] OPM officials left out the fact that Cylance and CyTech also identified malware related to the data breach. In the case of CyTech, CyFIR agents were deployed on April 21, 2015 to several production servers where CyFIR images were collected and transmitted to US-CERT. Subsequent analysis showed the presence of malicious files related to the data breach.[769]

Rep. Turner also asked Archuleta and Seymour whether Cytech was ever brought in to run a scan on OPM's equipment.[770] Seymour testified that "CyTech was engaged with OPM" and added that OPM was looking at using CyTech's tool on the OPM network.[771] She stated her understanding was that OPM "gave them some information to demonstrate whether their tool would find information on [OPM's] network, and that – in doing so, they did indeed find those indicators on OPM's network."[772] She testified:

> Seymour: [W]e had purchased licenses for CyTech's tool. We wanted to see if that tool set would also discover what we had already discovered. So, yes, they put their tools on our network, and yes, they found that information as well."
>
> Turner: So you were tricking them? You like already knew this, but you brought them in and said, Shazam, you caught it too? That seems highly unlikely, don't you think?
>
> Seymour: We do a lot of research before we decide on what tools we are going to buy for our network.
>
> Turner: At that point you hadn't removed the system from your system? I mean, you knew it was there, you brought them in, and their system discovered it too, which means it would have been continuously running, and that personnel information would have been still at risk. Correct?
>
> Seymour: No, Sir. We had latent malware on our system that we were watching that we had quarantined.

---

[150] *Id.*

[768] AAR Timeline – Unknown SSL Certificate (April 15, 2015), at HOGR020316-1922 (OPM Production: Apr. 29, 2016).

[769] U.S. Dep't of Homeland Security/US-CERT, Preliminary Digital Media Analysis-INC465355-A (May 4, 2015) at HOGR0724-001032 (OPM Production: Dec. 22, 2015); Briefing by U.S. Office of Pers. Mgmt. to H. Comm. on Oversight & Gov't Reform Staff (Apr. 18, 2016).

[770] *Hearing on OPM Data Breach: Part II.*

[771] *Id.*

[772] *Id.*

Turner: You had quarantined it. So it was no longer operating.

Seymour: That is correct.[773]

Seymour's testimony raised several questions. First, documents show OPM had not purchased licenses, or anything else, from CyTech—despite a verbal request for an emergency purchase order.[774]

Second, testimony obtained by the Committee shows CyTech was not given the indicators of compromise prior to running CyFIR on OPM's network on April 21, 2015. Documents obtained from OPM suggest indicators of compromise were shared with an OPM contractor Imperatis – on April 23, 2015 days after the April 21 CyTech demonstration.[775] An Imperatis employee escorted Cotton when he was onsite at OPM, but there is no evidence showing he provided Cotton or CyTech with indicators of compromise prior to the April 21 demonstration.

Third, Seymour's claim that the CyFIR tool identified "latent malware" on systems that had been quarantined is not accurate. Wagner testified the CyFIR tool was deployed in a live production environment.[776] Documents show OPM prioritized deployment of the CyFir tool to servers in the OPM production environment.[777] In fact, the CyFIR tool is designed to run in a live environment and runs against programs running in live memory.[778]

Seymour's claim that the malware in the OPM system had been quarantined is not accurate. Cotton testified: "there was no quarantine in place when I found the malware live on the system on the morning of the 22nd."[779] The agency did not move the primary tool used to identify malware enterprise-wide (CylanceProtect) from alert to auto-quarantine mode until April 24, 2015.[780] The CyFIR tool did in fact identify malware, and contrary to Seymour's testimony, the CyFIR tool did so in a live environment.[781]

Data on CyTech's CyFIR Appliance Collected During the 2015 Incident Response Period was Deleted

After two hearings in June 2015, the Committee requested additional information and documents from OPM related to the data breach incident announced in 2015, including specific

---

[773] *Hearing on OPM Data Breach: Part II* (Statement of Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt.).
[774] Wagner Tr. at 103.
[775] Cotton Tr. at 14, 16; Email from Brendan Saulsbury, Senior Cyber Security Engineer, SRA, to [redacted] Imperatis (April 23, 2015, 12:47 p.m.) at HOGR020316-000254 (OPM Production: Feb. 16, 2016) ([redacted] escorted Cotton for the April 21 demonstration).
[776] Wagner Tr. at 103.
[777] Message from [redacted] Contractor, U.S. Office of Pers. Mgmt., to Jonathan Tonda, Contractor, U.S. Office of Pers. Mgmt. (Apr. 28, 2015) at HOGR020316-000333 (OPM Production: Feb. 16, 2016).
[778] Cotton Tr. at 10.
[779] Cotton Tr. at 77.
[780] Saulsbury Tr. at 71; *see also* McClure Tr., Ex. 12.
[781] Wagner Tr. at 102.

information about CyTech and the use of the CyFIR tool at OPM. The Committee requested information about CyTech's role in this incident in a July 24, 2015 letter to OPM, then Chairman Chaffetz issued a preservation order to OPM on August 21, 2015, and on September 9, 2015, the Committee requested specific additional information about CyTech's tool, CyFIR, after learning data on the tool was deleted before it was returned to CyTech.[782]

Despite a clear obligation to preserve documents and evidence relevant to the Committee's investigation, OPM deleted data on CyTech's CyFIR appliance before returning the appliance to CyTech on August 20, 2015. The CyFIR appliance was used to collect forensic images that would assist the investigation of the data breach. Those images are relevant to determining the scope of the intrusion and data exfiltration.

OPM Retained CyTech's CyFIR Appliance Through August 2015

On June 23, 2015, HPSCI advised the Committee that OPM was still in possession of the CyFIR appliance.[783] Documents show that on June 25, 2015, OPM requested instructions from CyTech to "uninstall" the CyFIR agents.[784] CyTech subsequently requested that the CyFIR appliance be returned, but it was not returned until August 20, 2015—one day after Committee investigators visited CyTech's offices.[785]

In mid-August 2015, OPM deleted data on the CyFIR appliance and arranged to return it. On August 13, 2015, Imperatis, the OPM contractor that introduced CyTech to OPM, wrote Wagner and advised that CyTech wanted the CyFIR appliance and offered to help coordinate its return.[786] An OPM contractor who worked for Wagner on IT Security Operations wrote: "we need to scrub HDs [hard drives] prior to pick up."[787]

Before Returning the CyFIR Appliance OPM Deleted Key Data.

After some internal discussion about the best way to remove "sensitive OPM data" from the CyFIR appliance, Saulsbury and Tonda, two OPM IT security operations contract employees handling security operations, requested permission to "secure delete all sensitive OPM data from the CyFIR demo server including memory images, disk images, and any individual files or

---

[782] Letter from the Hon. Jason Chaffetz, Chairman and the Hon. Elijah E. Cummings, Ranking Member, H. Comm. on Oversight & Gov't Reform, to the Hon. Beth Cobert, Acting Dir., U.S. Office of Pers. Mgmt. (July 24, 2015); Letter from the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform and the Hon. Michael Turner, to the Hon. Beth Cobert, Acting Dir., U.S. Office of Pers. Mgmt. (Sept. 9, 2015).

[783] Letter from the Hon. Devin Nunes, Chairman and the Hon. Adam Schiff, Ranking Member, H. Perm. Select Comm. on Intelligence, to the Hon. Jason Chaffetz, Chairman and the Hon. Elijah E. Cummings, Ranking Member, H. Comm. on Oversight & Gov't Reform (June 23, 2015).

[784] Cotton Tr., Ex. 6 (Email from [redacted] Contractor, U.S. Office of Pers. Mgmt., to Juan Bonilla, Senior Sec. Consultant, CyTech (June 25, 2015).

[785] Cotton Tr. at 72.

[786] Email from Patrick Mulvaney, Imperatis, to Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt. (Aug. 13, 2015, 11:26 a.m.) at HOGR0909-000080-81 (OPM Production: Oct. 28, 2015).

[787] Email from Jonathan Tonda, Contractor, U.S. Office of Pers. Mgmt., to Patrick Mulvaney, Imperatis, and Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt. (Aug. 13, 2015, 11:41 a.m.) at HOGR0909-000080-81 (OPM Production: Oct. 28, 2015).

metadata extracted from OPM devices."[788] On August 17, 2015, Wagner approved this request.[789]

The process of deleting the data was tedious. On August 18, 2015, Saulsbury—who had been directed to delete the data on the CyFIR appliance—reported to his colleague Tonda that the "secure delete is only about 30% complete."[790] Saulsbury and Tonda were aware that the Committee was investigating the breach at this time. In an email, Saulsbury asked Tonda, "do you need help with anything for the HOGR stuff."[791] Tonda responded: "[N]ot yet. I'm reviewing it with Jeff now. Maybe later." So at the same time, the data on the CyFIR appliance was being deleted, they were aware that there were outstanding Committee requests for information. Nonetheless, OPM made the decision to delete the data on the CyFIR appliance.[792]

On August 19, 2015 (the same day that Committee investigators met with CyTech staff at their offices), a counsel from the OPM OIG told staff in the Office of General Counsel that CyTech was "complaining that OPM still has not returned the server/application thingee that CyTech built and left with OPM after the demonstration."[793] He further stated: "heard something that will create unpleasant work for both our offices unless it's headed off. . . . looks like a bad-publicity lawsuit coming down the pike unless, assuming of course that OCIO has it, OPM returns it. Just saying . . ."[794] Wagner forwarded this exchange to an Imperatis employee and said, "I want this [CyFir appliance] gone today."[795]

There is no evidence showing any OPM official recommended that the data on the CyFIR appliance should be preserved in light of the ongoing congressional investigation.

After the CyFIR appliance was returned on August 20, 2015, CyTech examined the appliance to determine what data was on the appliance for the purpose of responding to the Committee's requests for information. CyTech determined that 11,035 files and directories were deleted by OPM personnel or contractors on August 17, 18, and 19, 2015.[796] Cotton testified that

---

[788] Email from Brendan Saulsbury, Senior Cyber Security Engineer, SRA, to Jonathan Tonda, Contractor, U.S. Office of Pers. Mgmt. and Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt. (Aug. 17, 2015) at HOGR0909-000107 (OPM Production: Oct. 28, 2015).

[789] Email from Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt. to Jonathan Tonda, Contractor, U.S. Office of Pers. Mgmt. (Aug. 17, 2015, 2:00 p.m.) at HOGR0909-000107 (OPM Production: Oct. 28, 2015).

[790] Messages between Brendan Saulsbury and Jonathan Tonda, OPM IT Security Operations contractors (Aug. 18, 205) at HOGR0909-000151-52 (OPM Production: Oct. 31, 2015).

[791] *Id.*

[792] Email from Jeff Wagner, Dir. IT. Sec. Operations, U.S. Office of Pers. Mgmt. to Jonathan Tonda, Contractor, U.S. Office of Pers. Mgmt. (Aug. 17, 2015, 2:00 p.m.) at HOGR0909-000107 (OPM Production: Oct. 28, 2015).

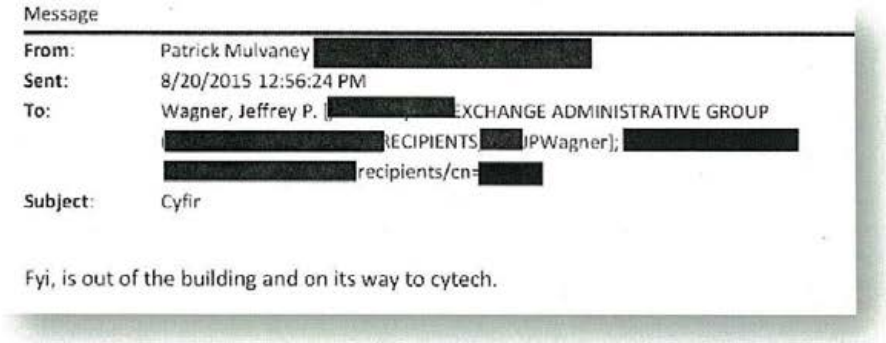
[793] Email from OIG Counsel, U.S. Office of Pers. Mgmt., to Associate Gen. Counsel, U.S. Office of Pers. Mgmt. (Aug. 19, 2015, 1:27 p.m.) at HOGR0909-000522 (OPM Production: Oct. 28, 2015).

[794] Email from OIG Counsel, U.S. Office of Pers. Mgmt., to Associate Gen. Counsel, U.S. Office of Pers. Mgmt. (Aug. 19, 2015, 1:27 p.m.) at HOGR0909-000522 (OPM Production: Oct. 28, 2015).

[795] Email from Jeff Wagner, Dir. IT. Sec. Operations, U.S. Office of Pers. Mgmt. to Patrick Mulvaney, Imperatis and Jonathan Tonda, Contractor, U.S. Office of Pers. Mgmt. (Aug. 19, 2015, 6:03 p.m.) at HOGR0909-000523 (OPM Production: Oct. 28, 2015).

[796] Cotton Tr., Ex. 12 (Forensics Report: OPM CyFIR Server Analysis Report (Sept. 10, 2015)). The Forensics Report included a 600 page Appendix A that listed in detail the 11,035 file names and any data or artifacts related to those files that was recoverable. Cotton Tr. at 74-75.

when CyTech examined the CyFIR device, they were interested in recovering certain database information in order to answer the Committee's questions and to provide clarity as to the scope of their activities while onsite at OPM in April-May 2015.[797] Cotton stated: "the CyFIR tool was not in a functioning state when it was returned to us."[798] Cotton also testified that the information on the CyFIR server would have been covered by the Committee's August 21, 2015 preservation order.[799]



Message

From: Patrick Mulvaney [redacted]

Sent: 8/20/2015 12:56:24 PM

To: Wagner, Jeffrey P. [redacted] EXCHANGE ADMINISTRATIVE GROUP [redacted] RECIPIENTS [redacted] JPWagner); [redacted] recipients/cn=[redacted]

Subject: Cyfir

Fyi, is out of the building and on its way to cytech.

OPM "Sanitized" the CyFIR Appliance

On October 28, 2015, OPM responded to the Committee's September 9, 2015 request for information about the CyFIR appliance.[800] The agency disclosed they "sanitized" the CyFIR appliance prior to returning it to CyTech.[801] The agency stated it did so in accordance with best practices and applicable information security policies[802]—without regard for the ongoing congressional investigation. The agency knew as of July 24, 2015 that there was an ongoing congressional investigation, and that CyTech's role in the data breach incident was a subject of the investigation.[803] Further, the Committee issued a preservation order related to the investigation on August 21, 2015.[804] The agency deleted the data on the appliance between August 17 and19, 2015.

---

[797] Cotton Tr. at 73.
[798] Cotton Tr. at 74.
[799] Cotton Tr. at 106.
[800] Letter from the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform and the Hon. Michael Turner, to the Hon. Beth Cobert, Acting Dir., U.S. Office of Pers. Mgmt. (Sept. 9, 2015); Letter from the Hon. Beth Cobert, Acting Dir. U.S. Office of Pers. Mgmt. to the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform and the Hon. Michael Turner (Oct. 28, 2015).
[801] Letter from the Hon. Beth Cobert, Acting Dir. U.S. Office of Pers. Mgmt. to the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform and the Hon. Michael Turner (Oct. 28, 2015).
[802] *Id.*
[803] Letter from the Hon. Jason Chaffetz, Chairman and the Hon. Elijah E. Cummings, Ranking Member, H. Comm. on Oversight & Gov't Reform, to the Hon. Beth Cobert, Acting Dir., U.S. Office of Pers. Mgmt. (July 24, 2015).
[804] Letter from the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform to the Hon. Beth Cobert, Acting Dir., U.S. Office of Pers. Mgmt. (Aug. 21, 2015).

OPM Violated the Anti-Deficiency Act

Documents and testimony show CyTech provided a service to OPM and OPM did not pay for this service. The Anti-deficiency Act (ADA) prohibits a federal agency from accepting voluntary services without obtaining an agreement in writing that the contractor will never seek payment.

The ADA's prohibition on accepting voluntary services

The ADA generally does not permit a federal agency or department to accept services from a contractor free of charge. The relevant section of the ADA states:

> An officer or employee of the United States Government or of the District of Columbia government may not accept voluntary services for either government or employ personal services exceeding that authorized by law except for emergencies involving the safety of human life or the protection of property.[805]

The ADA was enacted to prevent the use of voluntary services to avoid congressional scrutiny. The ADA, first passed in 1884 and substantially amended in 1950 and 1982, represented a desire to set strict limits on executive branch payroll and procurement officials.[806] Executive branch employees often worked overtime in excess of the agency's congressionally approved budgets, and the agency would subsequently request back pay for the employees.[807] Congress found it politically and morally problematic to deny payment to individuals who had rendered valuable services to the federal government—a fact the agencies well knew.[808] To eliminate this tactic for increasing departmental budgets, Congress prohibited voluntary services altogether.

The "gratuitous" services exception

While "voluntary" services are prohibited by the ADA, courts have distinguished "voluntary" services from "gratuitous" services. "Gratuitous" services are offered under an arrangement in which the government receives uncompensated services in accordance with an advance written agreement or contract in which the provider of the services agrees to serve without compensation.[809]

A contractor or individual can thus provide "gratuitous" services free of charge without violating the ADA so long as the contractor signs a written agreement in advance stating that the

---

[805] 31 U.S.C. § 1342 (2012).
[806] *See* Gov't Accountability Office, B-309301, *Recess Appointment of Sam Fox* (June 8, 2007).
[807] *Id.*
[808] *Id.*
[809] *Id.*

services are being offered without expectation of payment and waiving any future pay claims against the government.[810]

The "emergencies" exception

The ADA allows the federal government to benefit from personal services exceeding what is authorized by law in the event of "emergencies involving the safety of human life or the protection of property."[811]

The exception has historically been understood to require two factors in order to be invoked: (1) a "reasonable and articulable connection between the function to be performed and the safety of human life or the protection of property," and (2) "some reasonable likelihood that the safety of human life or the protection or property would be compromised, in some degree, by delay in the performance of the function in question."[812]

Previous successful invocations of the emergency exception have required a close nexus between the service being provided and the life or property protected. For example, the arbiter of ADA violations, the Government Accountability Office, found an exception when a municipal health officer disinfected a federal government compound to prevent the further spread of diphtheria that had already resulted in four deaths in that specific compound.[813]

When the service provided is merely convenient or helpful in avoiding a future emergency, it does not qualify under the exception. GAO ruled in 1930 that a man who offered to tow a Navy seaplane to a nearby island after a forced landing did not qualify under the emergency exemption.[814] GAO found the rendering of service to avoid a potential future emergency was not enough to invoke the exception.[815]

The ADA applied to the OPM and CyTech Situation

On April 21, 2015, CyTech provided a demonstration of its CyFIR tool at OPM's facility in Washington, D.C.[816] CyTech CEO Ben Cotton conducted the demonstration using CyTech equipment, most notably a computer forensics tool known as CyFIR.[817] For the demonstration, CyTech brought a CyFIR server to OPM, which would be connected to OPM's network and provide forensics services on up to twenty machines.[818]

---

[810] Gov't Accountability Off., B-324214, Decision, *Department of Treasury—Acceptance of Voluntary Services* (Jan. 27, 2014).
[811] 31 U.S.C. § 1342 (2012).
[812] 43 Op. Att'y Gen. 293, 302 (1981).
[813] 12 Com. Dec. 155 (Gov't Accountability Office 1905).
[814] 10 Com. Gen. 248 (Gov't Accountability Office 1930).
[815] 10 Com. Gen. 248 (Gov't Accountability Office 1930).
[816] OPM Visitor Log, Washington, D.C. (Apr. 21, 2015) at HOGR020316-000522 (OPM Production: Feb. 16, 2016).
[817] Email from [redacted] Imperatis, to Jeff Wagner, Dir. Info. Tech. Sec. Operations and Jonathan Tonda, Contractor, U.S. Office of Pers. Mgmt. (Apr. 20, 2015, 4:22 p.m.) at HOGR0909-000007 (OPM Production: Oct. 28, 2015).
[818] Cotton Tr. at 43.

CyTech expected to be paid

At that time, OPM had not purchased any licenses from CyTech. CyTech only provided a limited licensing arrangement for the purposes of the demonstration (for which typically there is no expectation of payment), to enable the installation of the CyFIR tool on twenty OPM machines for thirty days, thereby allowing the machines to be scanned for malware and unknown software processes. On April 22, 2015, Cotton reported the results of the demonstration to OPM staff and to [redacted] of Imperatis, another contractor retained by OPM.[819] The CyTech system had identified three unknown processes.[820] The results of the CyFIR scan were copied to a thumb drive and taken to OPM's security experts.[821]

Around noon that day, Cotton had a conversation with Jeff Wagner, OPM's Director of IT Security Operations, about the CyFIR findings. Wagner asked for a purchase order for the CyFIR tool that would cover 15,000 agents, six appliances, and 1,000 data analysts.[822] Cotton agreed to immediately expand the number of CyFIR licenses to 1,000 before a purchase order was formalized.[823] In this conversation with Wagner, Cotton also committed a CyTech expert to provide incident response and forensic support for the investigation.[824]

OPM's purchase order for CyTech services was to be made via a preexisting contract vehicle with Imperatis.[825] Consequently, Cytech provided a quote to Imperatis on April 24 for 15,000 CyFIR licenses, six CyFIR appliances, six training vouchers, and 1,040 onsite engineering support hours that would cost a total of $818,000.[826] In the meantime, CyTech, relying on the government's verbal request for services beyond a typical demonstration situation, began expanding its services to OPM and provided a license to OPM on April 22, 2015 for 1,000 endpoints that expired on June 30, 2015.[827]

The documents show specific incident response and forensic support activities that CyTech provided to OPM for which OPM should have compensated CyTech. The documents show OPM confirmed that the CyTech expert, Juan Bonilla, would be "assisting with an investigation over the next two weeks."[828] In terms of specific CyTech activities, Cotton

---

[819] Wagner Tr. at 102-103.
[820] Wagner Tr. at 102-103.
[821] Cotton Tr. at 19.
[822] Cotton Tr., Ex. 3, 4 (CyTech Price Quote ($818,000) for Emergency Purchase Order (Apr. 24, 2015) and CyTech [redacted] Transmittal email to Imperatis for CyTech Quote (Apr. 24, 2015)).
[823] Email from Ben Cotton, Chief Exec. Officer, CyTech to H. Comm. on Overisght & Gov't Reform Majority Staff (Apr. 16, 2016) (confirming the nature of the licensing arrangement as of April 22, 2015) (on file with the Committee).
[824] Cotton Tr. at 25. Cotton noted that CyTech's expert, Bonilla, as a senior member of the CyTech team, is typically billed at between $350 and $450 an hour. *Id.*
[825] Cotton Tr. at 23.
[826] Cotton Tr., Ex. 3, 4 (CyTech Price Quote ($818,000) for Emergency Purchase Order (Apr. 24, 2015) and CyTech [redacted] Transmittal email to Imperatis for CyTech Quote (Apr. 24, 2015)).
[827] Email from Ben Cotton, Chief Exec. Officer, CyTech to H. Comm. on Overisght & Gov't Reform Majority Staff (Apr. 16, 2016) (confirming the nature of the licensing arrangement as of April 22, 2015) (on file with the Committee).
[828] Email Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt. to IT Administration, U.S. Office of Pers. Mgmt. (Apr. 28, 2015) at HOGR020316-000707 (OPM Production: Feb. 16, 2016).

testified that CyTech was initially asked to image all the random access memory of about fifty computers and then image the hard drives for those computers and pull event logs for OPM.[829] CyTech also worked with Cylance, an OPM contractor, to fulfill their requests for files.[830]

Documents show CyTech's role in providing forensic support was significant—CyTech collected thousands of images in its forensic support role.[831] Documents show the agency continued to use the CyFIR tool in May 2015 through early June. For example, on May 7, 2015, Cylance requested deploying CyFIR to a particular OPM host machine.[832] In another email on June 1, 2015, an OPM contractor confirmed that "all other security agents are currently running, Cylan[c]e, CyFIR, Forescout . . . ."[833]

Documents show the agency and its contractor, Imperatis, expected OPM would be compensating CyTech for incident response and forensic support based on the conversations CyTech had with OPM in April 2015. For example, during the week of April 27, 2015, an Imperatis weekly report stated: "coordinating equipment installation and configuration with security vendors" including "working to finalize BOM [bill of materials]" for CyFIR.[834] Then, as late as June 5, 2015, Imperatis inquired about the status of the CyTech quote. An Imperatis employee emailed an OPM official: "do you want CyFIR for the existing network, I assume yes to compliment [*sic*] your Encase tool?"[835]

The documents show CyTech provided a demonstration, and following that demonstration, OPM requested a purchase order for CyTech services to support incident response activities, including forensic support. Based on the agency's apparent intent to finalize a purchase order, CyTech expanded the CyFIR licensing arrangement beyond what would normally be provided in a demonstration and provided onsite incident response services from April 23 through May 1, 2015. OPM also retained the CyFIR equipment for months after the demonstration, and used at least some of the licenses for CyFIR.[836] The record demonstrates CyTech was never compensated for these services and CyTech did not sign an agreement stipulating that its services would be provided for free.

---

[829] Cotton Tr. at 27-28.

[830] Email from Chris Coulter, Managing Dir., Cylance, to Ben Cotton, Chief Exec. Officer, CyTech (Apr. 24, 2015, 5:54 p.m.) at HOGR020316-000010 (OPM Production: Feb. 16, 2016).

[831] Email from Juan Bonilla, Senior Sec. Consultant, CyTech, to Brendan Saulsbury, Senior Cyber Security Engineer, SRA (Apr. 29, 2015, 5:26 p.m.) at HOGR020316-000043 (OPM Production: Feb. 16, 2016).

[832] Email from Chris Coulter, Managing Dir., Cylance, to Jonathan Tonda, Contractor, U.S. Office of Pers. Mgmt. (May 7, 2015, 3:56 p.m.) at HOGRO020316-000351 (OPM Production: Feb. 16, 2016).

[833] Email from Contractor, U.S. Office of Pers. Mgmt. to U.S. Office of Pers. Mgmt. Employees (June 1, 2015, 4:42 p.m.) at HOGR020316-000363 (OPM Production: Feb. 16, 2016).

[834] Imperatis Weekly Report (Apr. 27, 2015-May 1, 2015), Attach. 6 at 000758 (Imperatis Production: Sept. 1, 2015).

[835] Email from Patrick Mulvaney, Imperatis to Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt. (June 5, 2015, 8:51 p.m.) at HOGR0909-000046 (OPM Production: Oct. 28, 2015).

[836] *See* Email from Contractor, U.S. Office of Pers. Mgmt. to U.S. Office of Pers. Mgmt. Employees (June 1, 2015, 4:42 p.m.) at HOGR020316-000363 (OPM Production: Feb. 16, 2016). (OPM contractor listing CyFIR as a security tool running on an OPM server); *see also* List of Locations on which CyTech's CyFIR was Tested at HOGR0724-000320-321 (OPM Production Sept. 25, 2015).

The ADA prohibits a transaction of this nature. All the services that were unrelated to the product demonstration—including the provision of 1,000 additional licenses after the demonstration was over—should have been paid for. The agency also kept CyTech's CyFIR hardware for months after the demonstration. CyTech did not sign any written agreement that might have converted its voluntary services to gratuitous services because it expected to eventually receive payment.

This scenario raises the same concerns that the authors of the ADA had in mind when the bill was originally passed. The agency accepted a valuable service from a company that expected to be paid, but never was. The agency's actions placed the federal government in the uncomfortable position of either approving retroactive payment for voluntary services, or forcing CyTech—a small, disabled veteran owned business—to bear the sole burden for thousands of dollars in expenses incurred in good faith to help OPM respond to a significant cyber incident.

Chapter 6: Connections Between the 2014 and 2015 Intrusions

There has been significant public commentary on the source of the data breaches at OPM.[837] The Administration has "chosen not to make any official assertions about attribution."[838] Some Administration officials have hinted at the source behind the cyberattacks. Director of National Intelligence James Clapper has referred to China as "the leading suspect," stating "you have to kind of salute the Chinese for what they did."[839]

The documents and testimony gathered over the course of the investigation, as well as analysis of private sector threat research, show the data breaches discovered in 2014 and 2015 are likely connected, potentially coordinated campaigns by two threat actor groups. This conclusion is based on evidence that indicates the threat actors' "tactics, techniques, and procedures" (TTPs) and attack infrastructure share a common source or benefactor.

The documents show a broader campaign against federal workers associated with the hacking collective Axiom Threat Actor Group ("Axiom") and the threat actor Deep Panda. This conclusion is based on a multifactor analysis of the threat actors, and the tools they used to perpetrate the data breaches in 2014 and 2015:

- First, the data breach discovered in March 2014 was likely conducted by Axiom, based on the presence of Hikit malware and other TTPs associated with this group.

- Second, the data breach discovered in April 2015 was likely perpetrated by the group Deep Panda (a.k.a. Shell_Crew; a.k.a. Deputy Dog) as part of a broader campaign that targeted federal workers. This conclusion is based on commonalities in the 2015 adversary's attack infrastructure and TTPs common to other hacks attributed to Deep Panda, including attacks on Wellpoint/Anthem, VAE Inc., and United Airlines. However, the cyber intrusion and data theft announced by Anthem in 2015 is a separate

---

[837] Brian Krebs, *Catching Up on the OPM Breach,* KREBS ON SECURITY (June 15, 2015, 11:25 AM), available at: http://krebsonsecurity.com/2015/06/catching-up-on-the-opm-breach/; *see also* Ellen Nakashima, *U.S. Decides Against Publicly Blaming China for Data Breach*, WASH. POST, July 21, 2015, available at: https://www.washingtonpost.com/world/national-security/us-avoids-blaming-china-in-data-theft-seen-as-fair-game-in-espionage/2015/07/21/03779096-2eee-11e5-8353-1215475949f4_story.html.

[838] Ellen Nakashima, *U.S. Decides Against Publicly Blaming China for Data Breach*, WASH. POST, July 21, 2015, available at: https://www.washingtonpost.com/world/national-security/us-avoids-blaming-china-in-data-theft-seen-as-fair-game-in-espionage/2015/07/21/03779096-2eee-11e5-8353-1215475949f4_story.html (citing a Senior Administration Official).

[839] David Welna, *In Data Breach, Reluctance to Point the Finger at China*, NAT'L PUB. RADIO, July 2, 2015, http://www.npr.org/sections/parallels/2015/07/02/419458637/in-data-breach-reluctance-to-point-the-finger-at-china. Director Clapper's nod towards China as the perpetrator of the OPM data breaches gained credibility when the Chinese government arrested "a handful of hackers it says were connected with the breach." Ellen Nakashima, *Chinese Government Has Arrested Hackers it Says Breached OPM Database*, WASH.POST, Dec. 2, 2015, available at: https://www.washingtonpost.com/world/national-security/chinese-government-has-arrested-hackers-suspected-of-breaching-opm-database/2015/12/02/0295b918-990c-11e5-8917-653b65c809eb_story.html.

attack by a separate threat-actor group unrelated to the hack against OPM discovered in 2015.

- Third, both Axiom and Deep Panda are believed to be state-sponsored threat-actors supported by the same foreign government.[840]

- Fourth, based on these facts, the Committee finds that the 2014 and 2014/2015 cyber intrusions into OPM's networks were likely connected, possibly coordinated campaigns.

One Group, Several Names

There is an inherent challenge in associating a data breach to a particular hacking group, as threat researchers and governments do not have a common naming convention for cyber threat actors.[841]

Threat intelligence researchers generally name threat actor groups based on intrusions—called campaigns—that share common characteristics. Over time, analyses of campaigns performed by different firms may result in the same threat actor group being given multiple different names. Only later are these different names linked or identified as the same group. The groups that will be discussed in this report—Axiom, Deep Panda, Shell_Crew, Deputy Dog, APT6, etc.—were created by threat researchers. For instance, Crowdstrike researchers have relied on the naming convention of "Deep Panda" [842] while other groups term the same threat actor groups as: PinkPanther, Deputy Dog, Shell_Crew, APT17, Group 72, Black Vine, etc.[843]

Finally, because naming conventions of threat actors often revolve around intrusion campaigns rather than membership and affiliation, the analysis is unable to account for major changes to the threat actor group's membership, funding, TTPs, malware, or infrastructure over time. This may result in one group being misidentified as another or two actor groups being identified as one.

---

[840] Novetta, *Operation SMN: Axiom Threat Actor Group Report* at 8-9.

[841] See e.g. Brian Krebs, *Catching Up on the OPM Breach,* KREBS ON SECURITY (June 15, 2015, 11:25 AM), available at: http://krebsonsecurity.com/2015/06/catching-up-on-the-opm-breach/; Novetta, *Operation SMN: Axiom Threat Actor Group Report* at 8-9; ThreatConnect Research Team, OPM Breach Analysis, THREATCONNECT (June 5, 2015), available at: https://www.threatconnect.com/opm-breach-analysis/.

[842] Dmitri Alperovitch, Deep in Thought: Chinese Targeting of National Security Think Tanks, CROWDSTRIKE BLOG (July 7, 2014), http://www.crowdstrike.com/blog/deep-thought-chinese-targeting-national-security-think-tanks/.

[843] *DeepPanda or Shell Crew: Who is Behind the Cyber Attacks on US Networks*, RESEARCH MOZ (June 22, 2015), http://www.researchmoz.us/article/deeppanda-or-shell-crew-who-is-behind-the-cyber-attacks-on-us-networks; RSA Incident Response, *Emerging Threat Profile Shell Crew* 5 (Jan. 2014),https://www.emc.com/collateral/white-papers/h12756-wp-shell-crew.pdf. Note: A set of common characteristics in these groups' cyber campaigns and intrusions led to the belief that they are all actually the same group with several different names.

The 2014 Data Breach: The Unique Malware of the Axiom Group

The Axiom Group has been found responsible for a series of highly sophisticated cyber campaigns against public and private sector targets throughout the world in the last six years.[844] The definitive technical and behavioral report on Axiom's history and methods of attack was conducted by the threat research group at Novetta in 2014,[845] which found, in part, that the "Axiom threat group is a well-resourced, disciplined, and sophisticated subgroup of a larger cyber espionage group."[846]

The data breach at OPM in 2014, like other attacks perpetrated by Axiom, or one of its subgroups, involved the use of Hikit malware as the primary means of maintaining presence in OPM's environment.[847] **According to Novetta, Hikit malware is a "tool only seen used by Axiom."[848]**

Hikit malware is a sophisticated remote access tool (RAT) that offers attackers the ability to create covert backdoors into target computer networks and eventually take full control of target computer networks.[849] Hikit is purposefully built to evade detection and circumvent protections offered by firewalls and network monitoring tools.[850]

Similar to most sophisticated cyber intrusion campaigns, Hikit can be modified for tailored-use in a target's network, and optimized to operate within and take advantage of the vulnerabilities of the software, hardware, or operating system in the victim's environment.[851] Additionally, configuration files extracted to Hikit binaries indicate that command and control domains (C2) callbacks are tailored towards the geographic and network environment in which the target network is located. According to Novetta, "C2 domains will consistently be named and hosted in such a way that traffic appears legitimate, likely in an effort to fool network security operators of target organizations."[852]

DHS' OPM Incident Report from June 2014 positively identified the malware responsible for the 2014 intrusion as two variants of Hikit: Hikit A and Hikit B.[853] Hikit A and Hikit B differ primarily in the methods they use to communicate with their C2 servers. Hikit A uses a "unique 4-byte XOR key for each packet" while Hikit B "compresses its network traffic

---

[844] Novetta, *Operation SMN: Axiom Threat Actor Group Report* at 8-9.
[845] Novetta and the Cyber Security Coalition that conducted "Operation SMN" published an executive summary of the operation on October 15, 2014. The final report was released in November 2014 and is the product of an industry led effort to identify and disrupt a threat actor group.
[846] Novetta, *Operation SMN: Axiom Threat Actor Group Report*, at 4.
[847] H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Jeffrey P. Wagner (Feb. 18, 2016) at 31-32.
[848] Novetta, *Operation SMN: Axiom Threat Actor Group Report*, at 19.
[849] Novetta, *Operation SMN: Axiom Threat Actor Group Report*, at 28.
[850] Novetta, *Operation SMN: Axiom Threat Actor Group Report*, at 24-25.
[851] Novetta, *Operation SMN: Axiom Threat Actor Group Report*, at 4, 21. The Novetta report makes many references to HiKit customization by the Axiom group, and consider it a "tier 1" custom piece of malware. *Id.* at 4, 21.
[852] Novetta, *Operation SMN: Axiom Threat Actor Group Report* at 21.
[853] June 2014 OPM Incident Report at HOGR0818-001234.

with quicklz then it is XORed with a hash of 'matrix_password' concatenated with itself in a loop six times."[854]

The actors responsible for the 2014 intrusion used a wide variety of command and control servers (C2) throughout the entirety of the intrusion lifecycle.[855] Forensic investigators were able to identify C2 servers active and in use during 2014 by detailed, deep inspection of network traffic in and out of OPM's environment. Analysis of the Hikit malware used in the attack provided a granular, comprehensive picture of the command and control infrastructure that was created to support the campaign. The domains and IP addresses were hard-coded as call-back functions within the Hikit malware used in the campaign.

Hostname	IP Address	Hikit Variant	Function	C2 Domain	
[redacted]	[redacted]	Hikit A	Bandwidth Monitoring Server	lgemetic[.]suroot[.]com	[redacted]
[redacted]	[redacted]	Hikit A	[redacted] Server	bookservice[.]chatnook[.]com	[redacted]
[redacted]	[redacted]	Hikit A	Backup [redacted] Storage Manager	testimagecdn[.]servepics[.]com	[redacted]
[redacted]	[redacted]	Hikit A	[redacted] Network Performance Monitor	testimagecdn[.]servepics[.]com	[redacted]
[redacted]	[redacted]	Hikit A	[redacted] Server	testimagecdn[.]servepics[.]com	[redacted]
[redacted]	[redacted]	Hikit A	[redacted]	N/A	[redacted]
			Server		
[redacted]	[redacted]	Hikit B	[redacted] Server	www[.]maxcdns[.]com	[redacted]
[redacted]	[redacted]	Hikit B	[redacted] Server	www[.]edjecasts[.]com	[redacted]
[redacted]	[redacted]	Hikit B	[redacted] Server	statics[.]hopto[.]org	[redacted]

C2 Domains and IPs used in the 2014 intrusion and their associated Hikit malware counterparts[856]

Hikit malware is extremely unique to a specific threat actor group. Hikit is known as a "Tier 1" implant, which means that it is a custom piece of malware that can be strongly attributed to one particular threat actor group.[857] Axiom uses a variety of tools in varying stages of the intrusion cycle, which fall generally into four families: "These families of malware range in uniqueness from extremely common (Poison Ivy, Gh0st, ZXshell) to more focused tools used by

[854] *Id.*
[855] June 2014 OPM Incident Report at HOGR0818-001244 - 1245.
[856] June 2014 OPM Incident Report at HOGR0818-001244 - 1245.
[857] Novetta, *Operation SMN: Axiom Threat Actor Group Report* at 19.

Axiom and other threat groups directed by the same organization (Derusbi, Fexel) to tools only seen used by Axiom (ZoxPNG/ZoxRPC, Hikit)."[858]

The use of Hikit in the 2014 intrusion strongly indicates that a group associated with Axiom is responsible for the 2014 intrusion. Analysis by open-source threat researchers is consistent with this finding, attributing the attack to a state-sponsored actor;[859] the Novetta report highlights that the Axiom Group's targets – Asian and Western governments responsible for government records, journalists and media organizations, et. al.[860]

Hikit was first detected in 2011 and has evolved and developed into multiple versions since then.[861] Hikit splits into two generational variants: Hikit generation one, which dates back to 2011, and Hikit generation 2, which spans between 2011 and 2013.[862] Both generations of Hikit allow a great deal of functionality for threat actors. Once Hikit is dropped on a system, the attacker will have a variety of capabilities, including:

1. File management (upload and download).

2. Remote shell.

3. Network tunneling (proxying).

4. *Ad hoc* network generation (connecting multiple Hikit infected machines to create a secondary network on top of the victim's network topology).[863]

In addition to there being two generations of Hikit, there are also variants. All the malware found in 2014 were two variants of Hikit malware, termed Hikit A and Hikit B.[864] According to the 2014 DHS Incident Report, the Hikit malware:

> [A]llow[ed] the attackers to create a reverse shell from their C2 [command and control] servers into the infected systems in OPM's network from a remote location anywhere in the world. Wagner reaffirmed the Hikit malware was mostly used for persistence, or maintaining a presence at OPM, though keylogging activity was also observed.[865]

Effectively, the malware was used so that the hackers could "still use it to obtain entry into OPM's network.[866] Hikit in particular has shown to take particular advantage of poor

---

[858] Novetta, *Operation SMN: Axiom Threat Actor Group Report* at 19.
[859] ThreatConnect Research Team, OPM Breach Analysis, THREATCONNECT (June 5, 2015), https://www.threatconnect.com/opm-breach-analysis/.
[860] Novetta, *Operation SMN: Axiom Threat Actor Group Report* at 10.
[861] Novetta, *Hikit Analysis* at 1 (Nov. 2014), available at: https://www.novetta.com/wp-content/uploads/2014/11/HiKit.pdf
[862] *Id.*
[863] Novetta, *Operation SMN: Axiom Threat Actor Group Report* at 27
[864] Saulsbury Tr. at 17.
[865] Wagner Tr. at 17.
[866] Saulsbury Tr. at 18.

internal firewalls and network segmentation.[867] According to one of the earliest analyses of Hikit malware conducted by FireEye, Inc., an attacker was able to tunnel via Remote Desktop and proliferate across the network using previously compromised credentials.[868] This allowed attackers to "create 'hop points' among internal and external network segments" by installing copies of the rootkit in strategic locations to establish new footholds within the target network.[869]

The Hikit malware was well-suited for use on OPM's network. DHS found OPM did not (and may still not) "have tiered network architecture with segmentation between users, databases, applications, and webservers. OPM's network is extremely flat at this time and has little to no segmentation."[870] DHS ultimately recommended: "the server environment should be segmented via firewalls into logically separate internally and externally accessible DMS, web server, application server, and database environment."[871] **The flat network architecture that OPM's legacy environment employed made the agency an ideal target for exploitation by the Hikit malware.**

Malware Discovered during the 2015 Data Breach

Security researchers have suggested a variety of possible threat actors are responsible for the 2015 data breach at OPM.[872] While much of the evidence that would support attribution of the actor to a particular threat actor or actors remains classified, public source documents indicate a group referred to as "Deep Panda" is likely to have been involved based on the attack infrastructure.[873]

Unlike the 2014 data breach, where Hikit malware could be uniquely linked to the Axiom Group, the use of PlugX malware in the 2015 data breach alone is not sufficient to positively identify "Deep Panda" as the culprit. The PlugX employed by the 2015 attackers is commonly used by cyber threat actors and has only become more prevalent since the initial

---

[867] Saulsbury Tr. at 18.

[868] Christopher Glyer & Ryan Kazanciyan, *The "Hikit" Rootkit: Advanced and Persistent Attack Techniques (Part 2)*, FIREEYE (Aug 22, 2012), available at: https://www.fireeye.com/blog/threat-research/2012/08/hikit-rootkit-advanced-persistent-attack-techniques-part-2.html.

[869] *Id.*

[870] June 2014 OPM Incident Report at HOGR0818-001236.

[871] *Id.*

[872] Jeremy Wagstaff, *Hunt for Deep Panda Intensifies in Trenches of U.S.–China Cyberwar*, REUTERS, June 21, 2015, available at: http://www.reuters.com/article/us-cybersecurity-usa-deep-panda-idUSKBN0P102320150621 ("Security researchers have many names for the hacking group that is one of the suspects for the cyberattack on the U.S. government's Office of Personnel Management: PinkPanther, KungFu Kittens, Group 72 and, most famously, Deep Panda. But to Jared Myers and colleagues at cybersecurity company RSA, it is called Shell Crew."); *see also* David Perera, *Agency Didn't Encrypt Feds' Data Hacked by Chinese*, POLITICO (June 4, 2015), available at: http://www.politico.com/story/2015/06/personal-data-of-4-million-federal-employees-hacked-118655 ("The massive data breach there affected the records of 4.1 million current and former federal employees and may be linked to a Chinese state-backed hacker group known as "Deep Panda," which recently made similarly large-scale attacks on the health insurers Anthem and Premera.").

[873] RSA Incident Response, *Emerging Threat Profile: Shell_Crew* 5 (2014),available at: https://www.emc.com/collateral/white-papers/h12756-wp-shell-crew.pdf.

intrusion in 2014.[874] An analysis of the infrastructure used to hack OPM's network in 2015, however, points toward the likely responsible actor. The adversary's attack infrastructure, which includes the websites used to hack OPM's networks and exfiltrate data, was similar to attack infrastructure used in seemingly unrelated cyber intrusions.

The malicious domains registered for the OPM hack had three distinct characteristics: Marvel comic book superhero names, GMX "throw away" e-mail accounts, and domain names tailored to appear as legitimate portions of OPM's network and training resources.[875] An advanced persistent threat's (APT) attack infrastructure is visible to cybersecurity experts in the form of domain names and their corresponding IP address hosted on C2 servers.[876] How, when, and by whom domain names and IP addresses are created, registered, and used in conducting a cyberattack are therefore important factors in attributing a hack to a particular actor. The adversary that perpetrated the data breach against OPM in 2015 used an attack infrastructure similar to cyberattacks tied to Deep Panda.

Cybersecurity research firms Crowdstrike and ThreatConnect have exposed a number of characteristics of Deep Panda's attack infrastructure.[877] These characteristics were identified during the analysis of several intrusions, including attacks on Wellpoint/Anthem,[878] VAE Inc.,[879] and United Airlines.[880] These attacks bear a striking similarity to the 2015 data breach at OPM.[881] The attacks share several common elements:

- Registrant Names: Domains were registered under names associated with Marvel's Avengers, or actors related to the *Iron Man* franchise and Marvel universe.

---

[874] Chris Brook, *PlugX, Go-to Malware for Targeted Attacks, More Prominent Than Ever*, THREATPOST, (Feb. 10, 2015), available at: https://threatpost.com/plugx-go-to-malware-for-targeted-attacks-more-prominent-than-ever/110936/

[875] ThreatConnect Research Team, *OPM Breach Analysis*, THREATCONNECT (June 5, 2015), available at: https://www.threatconnect.com/opm-breach-analysis/.

[876] Wagner testified that one of the reasons he considered the 2015 attackers to be sophisticated was because "[the 2015 attackers] used specifically U.S.-based IP hosting addresses to prevent geolocation rules from being effective." Wagner Tr. at 132.

[877] Threat Connect Research Team, *The Anthem Hack: All Roads Lead to China*, THREATCONNECT (Feb. 27, 2015), available at: https://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/; *see also* Matt Dahl, *I am Ironman: DEEP PANDA Uses Sakula Malware to Target Organizations in Multiple Sectors*, CROWDSTRIKE BLOG (Nov. 24, 2014), available at: http://www.crowdstrike.com/blog/ironman-deep-panda-uses-sakula-malware-target-organizations-multiple-sectors/?_ga=1.192876841.2030632883.1465319953.

[878] Drew Harwell & Ellen Nakashima, *China Suspected in Major Hacking of Health Insurer*, WASH. POST, Feb. 5, 2015, available at: https://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?tid=a_inl.; Elizabeth Weise, *Massive Breach at Health Care Company Anthem Inc.,* USA TODAY, Feb. 5, 2015, available at: http://www.usatoday.com/story/tech/2015/02/04/health-care-anthem-hacked/22900925/.

[879] Ellen Nakashima, *Security Firm Finds Link Between China and Anthem Hack*, WASH. POST, Feb. 27, 2015, https://www.washingtonpost.com/news/the-switch/wp/2015/02/27/security-firm-finds-link-between-china-and-anthem-hack/.

[880] Threat Connect Research Team, *The Anthem Hack: All Roads Lead to China*, THREATCONNECT (Feb. 27, 2015), available at: https://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/.

[881] *Id.*

- Registrant Emails: The domains were registered using emails that were a combination of pseudorandom ten-digit alphanumeric usernames and "@gmx[.]com" e-mail accounts.[882]

- Faux Domain Names: Registered domains were tailored to look like legitimate domains hosting resources that belonged to the target organization, or portions of the target's network.[883]

With respect to registrant names, Deep Panda's use of a comic book themed naming convention was previously documented by Crowdstrike during their analysis of a 2014 campaign against, among other targets, the healthcare and government sectors.[884] The agency, using a variety of network monitoring tools, identified three domains as the primary attack infrastructure: opmsecurity.org; wdc-news-post.com; and opm-learning.org.

Malicious Domain	Malicious Registrant	Origional Registrant Email	Associated Incident
opm-learning[.]org	tony stark	vrzunyjkmf@gmx[.]com	OPM Breach
opmsecurity[.]org	Steve Rogers	tAPRhpALhl@gmx[.]com	OPM Breach
wiki-vaeit[.]com	Tony Stark	EwibAFNxEe@gmx[.]com	VAE, Inc. Targeting Campaign
sharepoint-vaeit[.]com	Natasha Romanoff	yXDlqMRNdM@gmx[.]com	VAE, Inc. Targeting Campaign
ssl-vaeit[.]com	Dubai Tycoon	aArwcsyHFb@gmx[.]com	VAE, Inc. Targeting Campaign
ssl-vait[.]com	John Nelson	aArwcsyHFb@gmx[.]com	VAE, Inc. Targeting Campaign
marsale[.]net	Mark Wahlberg	eumyjxkywn@gmx[.]com	Unidentified
united-airlines[.]net	James Rhodes	enijswwxsk@gmx[.]com	Unidentified

ThreatConnect chart shows similar registrant names, e-mails, and domains—evidence of a larger, more complex campaign[885]

Deep Panda registered their attack infrastructure using the names of Marvel's Avengers characters and other names associated with the film franchise:

- Tony Stark (a.k.a. Iron Man).

- Steve Rogers (a.k.a. Captain America).

- Natasha Romanoff (a.k.a. Black Widow).

- James Rhodes (a.k.a. War Machine).

- John Nelson (the visual effects supervisor for the Marvel film *Iron Man*).[886]

---

[882] *OPM Breach Analysis: Update*, THREATCONNECT (last visited June 15, 2016), https://www.threatconnect.com/opm-breach-analysis-update/.
[883] Threat Connect Research Team, *The Anthem Hack: All Roads Lead to China*, THREATCONNECT (Feb. 27, 2015), available at: https://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/.
[884] Matt Dahl, *I am Ironman: DEEP PANDA Uses Sakula Malware to Target Organizations in Multiple Sectors*, CROWDSTRIKE BLOG (Nov. 24, 2014), available at: http://www.crowdstrike.com/blog/ironman-deep-panda-uses-sakula-malware-target-organizations-multiple-sectors/?_ga=1.192876841.2030632883.1465319953.
[885] ThreatConnect Research Team, *OPM Breach Analysis*, THREATCONNECT (June 5, 2015), available at: https://www.threatconnect.com/opm-breach-analysis/.
[886] *John Nelson Biography*, IMDB, available at: http://www.imdb.com/name/nm0625471/?ref_=fn_al_nm_1.

- Dubai Tycoon (the name of an uncredited role in the Marvel film *Iron Man* portrayed by noted rapper and Wu-Tang Clan member Ghostface Killah).[887]

With respect to registrant email addresses and domain names, the original registrant's email was always a random alphanumeric with a @gmx.com email address, and the domains had OPM themed names.

On April 25, 2014, actors registered the malicious domain "opmsecurity.org," under the name "Steve Rogers" using the e-mail address "tAPRhpALhl@gmx.com."[888] Shortly after the "Big Bang" concluded and just eighteen days after the *New York Times* broke news of the breach on July 9, 2014,[889] another OPM-themed C2 node was established by the same actors. On July 29, 2014, the attackers registered the OPM-themed domain "opm-learning[.]org." The domain was registered by "Tony Stark" using the e-mail address "vrzunyjkmf@gmx[.]com."[890]

In addition, Deep Panda's attack infrastructure typically involves domain names tailored to look like legitimate domains that belong to the target organization.[891] For instance, the security firm ThreatConnect has tied the use of "Wellpoint look-alike domains to a series of targeted attacks launched in May 2014 that appeared designed to trick Wellpoint employees into downloading malicious software tied to the Deep Panda hacking gang."[892]

Domains such as we1lpoint.com or myhr.we1lpoint.com were used in the course of a campaign against Anthem.[893] Security expert Brian Krebs stated: "[It] appeared that whoever registered the domain was attempting to make it look like 'Wellpoint,' the former name of Anthem before the company changed its corporate name in late 2014."[894] These victim-centric domains could easily fool network monitors as they, at first glance, appear legitimate, but under further analysis are proven to be malicious.

---

[887] *Iron Man Trivia*, IMDB, http://www.imdb.com/title/tt0371746/trivia (last visited June 30, 2016). ("Ghostface Killah, a long-time fan of the Iron Man comics (he uses the aliases 'Ironman' and 'Tony Starks,' titled his 1996 album 'Ironman' and sample clips of Iron Man (1966)), had a cameo as a Dubai tycoon. However, his scene was cut from the final film. Jon Favreau apologized to Ghostface and used his "We Celebrate" video in the film.").

[888] *OPM Breach Analysis: Update*, THREATCONNECT (last visited June 15, 2016), available at: https://www.threatconnect.com/opm-breach-analysis-update/.

[889] Michael S. Schmidt, David E. Sanger & Nicole Perlroth, *Chinese Hackers Pursue Key Data on U.S. Workers*, N.Y. TIMES, July 9, 2014, http://www.nytimes.com/2014/07/10/world/asia/chinese-hackers-pursue-key-data-on-us-workers.html?_r=0.

[890] *OPM Breach Analysis: Update*, THREATCONNECT, available at: https://www.threatconnect.com/opm-breach-analysis-update/.

[891] Threat Connect Research Team, *The Anthem Hack: All Roads Lead to China*, THREATCONNECT (Feb. 27, 2015), available at: https://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/.

[892] Brian Krebs, *Premera Blue Cross Breach Exposes Financial, Medical Records*, KREBS ON SECURITY (Mar. 17, 2015, 5:42 PM), available at: http://krebsonsecurity.com/2015/03/premera-blue-cross-breach-exposes-financial-medical-records/#more-30380.

[893] Threat Connect Research Team, *The Anthem Hack: All Roads Lead to China*, THREATCONNECT (Feb. 27, 2015), available at: https://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/.

[894] Brian Krebs, *Anthem Breach May Have Started in April 2014*, KREBS ON SECURITY (Feb. 15, 2015, 10:34 AM), available at: http://krebsonsecurity.com/2015/02/anthem-breach-may-have-started-in-april-2014/.

Deep Panda also appeared to name the domains to emulate portions of the target's network or to mimic organizationally-related resources hosted outside the target's network.[895] In the case of VAE, Deep Panda made the domains look like company-related Sharepoint or Wiki resources by naming them "sharepoint-vaeit.com" and "wiki-vaeit.com."[896] In the 2015 OPM breach, the malicious domains used for command and control, "opm-learning[.]org" and "opmsecurity.org," resemble the websites OPM uses for its annual information technology security awareness training, "opmsecurity.golearning.org" and "security.golearnportal.org."[897] This training is required for all full-time and part-time federal employees and contractors who have access to OPM's networks.[898]

The faux-domain naming used in these hacks is a Deep Panda "calling card," but it also reveals information about Deep Panda's TTPs. These victim-centric domains could slip past network monitors as they, at first glance, appear legitimate. The domains are designed to fool employees into thinking they are legitimate. After clicking on a link sent through a spear phishing e-mail, attackers can download malware into the company's network by exploiting vulnerabilities in the victim's web browser. This technique, called a "watering hole attack,"[899] is a strategy that uses hacked websites or fake, legitimate-looking domains to download malware into a victim's computer.[900] Watering hole attacks are a technique heavily favored by, though not exclusive to, the Deep Panda threat actor group.[901]

Another common element of Deep Panda's campaigns is it often relies on some of the same attack infrastructure for multiple intrusions, including the breach into OPM's network.[902] The following domains were active on OPM's systems during the course of incident response:[903]

Entry #	IP	Domain
Entry 1	[redacted]	Wiki-vaeit.com Sharepoint-vae.com ssl-vaeit.com Wiki-vaeit.com
Entry 2	[redacted]	We1lpoint.com

[895] Threat Connect Research Team, *The Anthem Hack: All Roads Lead to China*, THREATCONNECT (Feb. 27, 2015), available at: https://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/.
[896] *Id.*
[897] *OPM Breach Analysis: Update*, THREATCONNECT (last visited June 15, 2016), available at: https://www.threatconnect.com/opm-breach-analysis-update/.
[898] Saulsbury Tr. at 34.
[899] So named because it resembles a strategy employed by predators, who will lie in wait to ambush prey at a site they are known or expected to frequent like a watering hole.
[900] Will Gragido, *Lions at the Watering Hole – The "VOHO" Affair*, RSA, (Jul 20, 2012), https://blogs.rsa.com/lions-at-the-watering-hole-the-voho-affair/
[901] Adam Greenberg, *Watering Hole Attacks are Becoming Increasingly Popular, Says Study*, SC MAGAZINE, Sept. 27, 2013, available at: http://www.scmagazine.com/watering-hole-attacks-are-becoming-increasingly-popular-says-study/article/313800/ (quoting Nick Levay, chief security officer with Bit9, "Watering holes have been on the rise in the past few years and a lot of hackers that were using spear phishing attacks to target people have started using watering holes,' said Levay, explaining that while watering holes typically target a specific group or community, he has seen narrower variants that, for example, will only target a certain range of IP addresses.")
[902] *See e.g.* ThreatConnect Research Team, *OPM Breach Analysis*, THREATCONNECT (June 5, 2015), available at: https://www.threatconnect.com/opm-breach-analysis/.
[903] OPM Domain Name Log (Unredacted) at HOGR0724-D00893-95-UR (OPM Production: Dec. 22, 2015).

		Extcitrix.wel1point.com Myhr.wel1point.com Hrsolultions.wel1point.com
Entry 3	[redacted]	drongobast.com efuelia.com gandaband.com kopirabus.com macroxaz.com mustufacka.com ns1.figaina5.com ns8.figaina5.net nsa.figaina5.net
Entry 4	[redacted]	nsa.org.cn
Entry 5	[redacted]	cdn.servehttp.com smtp.outlookssl.com

Entries 1 and 2 in the above chart are malicious domains also used by Deep Panda against VAE and Wellpoint/Anthem systems.[904] Seven of these domains (Wiki-vaeit.com, Sharepoint-vae.com, ssl-vaeit.com, We1lpoint.com, Extcitrix.wel1point.com, Myhr.wel1point.com, Hrsolultions.wel1point.com) were active on OPM's systems during the 2015 data breach and share common identifiers with the primary infrastructure used to perpetrate the breach against OPM discovered in 2015, including Avengers-themed names and GMX email addresses. Threat researchers tied attacks at VAE and Anthem to a "group known by a number of names, including Deep Panda, Axiom, Group 72, and the Shell_Crew."[905]

Testimony shows OPM security personnel also connected the 2015 attack to Deep Panda. Saulsbury testified:

> Q. So my question is as a result of the April 2015 cyber intrusion, was OPM SOC able to draw any conclusions as to whom or what organization might have been responsible for the malicious activity? And again, to the extent you can answer without revealing any classified information.
>
> A. Right, so to clarify, I do not have a clearance. I do not have access to any classified information. The only unclassified information that we have was that some of those Marvel character-related domain names or domain registrants, they showed up in a -- I believe it was a Mandiant report, incident response report regarding a publicized data breach for a healthcare provider, but I can't recall specifically which it was at this time. But the Mandiants dubbed the attacker Deep Panda, (emphasis added) so

[904] Threat Connect Research Team, *The Anthem Hack: All Roads Lead to China*, THREATCONNECT (Feb. 27, 2015), available at: https://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/.
[905] Brian Krebs, *Anthem Breach May Have Started in April 2014*, KREBS ON SECURITY (Feb. 15, 2015, 10:34 AM), available at: http://krebsonsecurity.com/2015/02/anthem-breach-may-have-started-in-april-2014/.

based on that domain registrant correlation, that is the only indication, or at least on the unclassified side, that we have that that may be the same attacker.[906]

Saulsbury's testimony was corroborated by Coulter, who testified about the Plug X malware and other evidence Cylance found on OPM's systems. Coulter stated:

A. So I'll use the word 'actor,' the ones that were identified in prior exhibits. You had Shell Crew, or sometimes known as Deep Panda, as well as Deputy Dog, and it has many, many other names. So those were the two that, at least as it relates to the industry research being done, that the malware that we found was closest related to it. By no means are we saying it was them; it's just it was a relationship or similarity.

Q. Okay. Are those two generally associated with a particular country?

A. In the industry, yes.

Q. Can I ask which country?

A. [redacted][907]

The 2015 OPM attackers' use of malicious domains similar to, or even the same as, those used in attacks against VAE and Wellpoint (Anthem) show Deep Panda likely perpetrated the data breach against OPM that was discovered in 2015. The similarities in the pseudorandom 10-digit GMX address, OPM-themed domains, and Avengers-themed registrants are evidence that the infrastructure was created and utilized by the same group. Documents and testimony connect Deep Panda and Axiom, and therefore the 2014 and 2015 data breaches at OPM were likely connected, and possibly coordinated.

2014 & 2015: Likely Connected, Possibly Coordinated

While OPM has maintained the cyberattacks conducted against their systems in 2014 and 2015 were separate occurrences, documents and testimony show a broader campaign against the information of federal workers by state-sponsored hacking organizations (Deep Panda and Axiom) were responsible.

Under a theory advanced by threat researcher FireEye, "many seemingly unrelated cyber-attacks may, in fact, be part of a broader offensive fueled by a shared development and logistics

[906] Saulsbury Tr. at 83.
[907] Coulter Tr. at 93.

infrastructure – a finding that suggests some targets are facing a more organized menace than they realize."[908]

The overlapping use of malware and exploits, or as FireEye called it, a "shared malware-builder tool,"[909] by Axiom and Deep Panda show the data breaches at OPM in 2014 and 2015 were likely connected, possibly coordinated.

If FireEye's theory is true, either Axiom and Deep Panda's efforts to collect data from OPM's systems in 2014 and 2015 were connected via a common supplier of cyber resources, or that Axiom and Deep Panda's efforts were actively coordinated by that supplier. While FireEye terms this common-supplier a "digital quartermaster," other threat researchers have identified a similar shared resources model. A researcher at PricewaterhouseCoopers LLP stated:

> In our experience, very few attackers have the patience to maintain completely distinct infrastructure with multiple registrars, name servers and hosting providers at the same time . . . in our view, the hypothesis with the highest probability is that groups of attackers share resources leading to overlaps – this appears to be an ever more common feature – with malware families, builders, and even sometimes hosting infrastructure being shared between disparate actors with a common goal.[910]

Documents show Axiom used Hikit malware to attack OPM's network in 2014 and were targeting the background investigation data stored on the PIPS system that was eventually stolen by Deep Panda using PlugX malware. Documents show Axiom and Deep Panda had more in common than their target.

Both have been tied to the use of Plug X and Hikit malware.[911] Among the challenges in making this assertion are the naming conventions used by the threat researcher community in analyzing data breaches and persistent threat actors. For example, threat researchers at Cisco stated that "hikit, according to our data [is] unique to Group 72 and to two other threat actor groups." Group 72 is an alias associated with a state-sponsored "espionage" group known by a number of names, including Deep Panda."[912] But Hikit is not the only malware that Axiom and

---

[908] FireEye, *Supply Chain Analysis: From Quartermaster to SunshopFireEye* at 3, available at: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-malware-supply-chain.pdf.
[909] *Id.*
[910] Chris Doman & Tom Lancaster, *ScanBox Framework – Who's Affected, and Who's Using It?*, PWC (Oct. 27, 2014), available at: http://pwc.blogs.com/cyber_security_updates/2014/10/scanbox-framework-whos-affected-and-whos-using-it-1.html.
[911] FireEye, *Supply Chain Analysis: From Quartermaster to SunshopFireEye* at 3, available at: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-malware-supply-chain.pdf
[912] Brian Krebs, *Anthem Breach May Have Started in April 2014*, KREBS ON SECURITY (Feb. 15, 2015, 10:34 AM), available at: http://krebsonsecurity.com/2015/02/anthem-breach-may-have-started-in-april-2014/ (It is noteworthy that Brian Krebs links Deep Panda and Axiom); *see also* Andrea Allievi et al, Cisco, *Deconstructing and Defending Against Group 72*, (2014), available at: http://www.talosintel.com/files/publications_and_presentations/papers/Cisco_security_Group72_wp.pdf.

Deep Panda use:[913]

Malware Name	Deep Panda	Axiom
Gh0st Rat (Moudour, Mydoor)	X	X
Poison Ivy (Darkmoon, Breut)	X	X
HydraQ (9002RAT, McRAT, Naid, Roarur, Mdmbot)	X	X
ZxShell (Sensode)	X	X
Deputy Dog (Fexel)	X	X
Derusbi	X	X
PlugX (Thoper, Sogu, Korplug, Kaba, DestroyRAT)	X	X
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
Sakula (Sakura, Sakurel)	X	
Mivast RAT	X	
Hurix	X	

In addition to an overlapping repertoire of malware, Axiom and Deep Panda have both been linked to the use of the "Elderwood Framework."[914] Symantec Security Response identified attackers employing "re-use components of an infrastructure" which they named the "Elderwood Framework," after "a source code variable used by the attackers."[915] The Elderwood Framework is effectively a library of exploits that hackers can use to conduct malicious operations.[916] Novetta cited Axiom's use of similar TTPs, tools, and other attack infrastructure, including "Elderwood platform attacks," in 2011, 2012, and 2014.[917] According to Symantec, "Black Vine," a.k.a. Deep Panda, also used the Elderwood Framework.[918]

The overlapping TTPs, malware, and attack infrastructure that Axiom and Deep Panda use suggests these groups share a "digital quartermaster," a central supplier of malicious tools, tactics, and techniques to a variety of state-sponsored espionage groups. This explains why the same group of hackers has launched attacks under several different names—Axiom, Deep Panda, Shell_Crew, Deputy Dog, etc.

With respect to the OPM breach, the attack infrastructure and common malware indicates Axiom and Deep Panda are probably connected. The overlapping timeframe of the attacks on OPM also suggest that a connection between the perpetrators.

---

[913] *See*, Novetta, *Operation SMN: Axiom Threat Actor Group Report*, at 4; s*ee also*, ThreatConnect Research Team, *OPM Breach Analysis*, THREATCONNECT (June 5, 2015), https://www.threatconnect.com/opm-breach-analysis/. *See also,* Brian Krebs, *Anthem Breach May Have Started in April 2014*, KREBS ON SECURITY (Feb. 15, 2015, 10:34 AM), http://krebsonsecurity.com/2015/02/anthem-breach-may-have-started-in-april-2014/, *See also,* Liam Tung, *Anthem Health Insurance Hackers are a Well-Funded, Busy Outfit*, CSO, July 29, 2015, http://www.cso.com.au/article/580685/anthem-health-insurance-hackers-well-funded-busy-outfit/.

[914] Gavin O'Gorman & Geoff McDonald, Symantec, *The Elderwood Project* (last visited June 15, 2016), http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf.

[915] *Id.*

[916] *Id.*

[917] Novetta, *Operation SMN: Axiom Threat Actor Group Report* at 12.

[918] Liam Tung, *Anthem Health Insurance Hackers are a Well-Funded, Busy Outfit*, CSO, July 29, 2015, available at: http://www.cso.com.au/article/580685/anthem-health-insurance-hackers-well-funded-busy-outfit/.

Documents show that while OPM was monitoring the 2014 attacker's movements in May 2014, the 2015 attackers were able to drop PlugX malware onto servers connected to the background databases the 2014 attackers were targeting.[919] Within forty-five days of their initial entry into OPM's networks, the 2015 attackers were able to gain access to the personnel records and background investigation databases, establish a "late-stage" attack infrastructure, and begin data exfiltration.

The speed at which the 2015 attackers were able to escalate access from initial entry to end-stage presence and exfiltration suggests a level of familiarity with OPM's environment. This creates the appearance that the 2015 attackers relied on information obtained by the 2014 hackers, who had access to OPM's network for years and were unable to compromise the most sophisticated systems, such as those holding background investigation data.

According to Saulsbury, the documents the 2014 attacker exfiltrated from OPM provided an attacker - or any associated group with (directly or indirectly) - an advantage.[920] As Mr. Saulsbury explained the documents provide "more familiarity with how the systems are architected. Potentially some of these documents may contain accounts, account names, or machine names, or IP addresses, which are relevant to these critical systems."[921]

The documents the 2014 attackers stole may be characterized as documents that provide overviews of key systems (such as PIPS, EPIC/eQIP, and Fingerprint Transactional System) and provide information as to who has access to those systems.[922] The documents effectively provide a roadmap to how the background and personnel data is ingested into OPM's systems, how OPM integrates those systems with the government contractors working on them, and who has access to those systems. It is the kind of information that would accelerate an attacker's familiarity with OPM's most highly sensitive information and could explain the speed with which the 2015 attacker was able to establish access, orient themselves, escalate network authorities, and penetrate the most highly sensitive data repositories on OPM's network.

Documents obtained by the Committee show additional evidence of a connection between the 2014 attacker and the 2015 attack. For example, the 2015 attacker persisted in their intrusion even after the public announcement of the 2014 data breach on July 9, 2014, and continued exfiltrating OPM's background investigation data. This shows the 2015 attackers had sufficient awareness of OPM's security protocols and were not worried despite the heightened state of security that was put in place. This suggests a degree of collusion or shared tasking between the two attackers, enough so that the 2015 attacker would be comfortable that earlier efforts would pave the way and the subsequent mitigation steps taken by OPM would not disrupt the 2015 attackers' ongoing operation.

Regardless of the names of the threat actor groups that were conducting malicious activity on OPM's systems it should have been clear to OPM in the wake of the 2014 data breach

[919] June 9, 2015 DMAR at HOGR0724-001154.
[919] June 2014 OPM Incident Report at HOGR0818 -001245.
[921] Saulsbury Tr. at 27-28.
[922] June 2014 OPM Incident Report at HOGR0818 -001245.

that they were facing a sophisticated, well-resourced adversary with connections to a spectrum of state-sponsored threat actors. Private sector threat researchers were connecting the dots between the targeted campaign against federal employees, as evidenced by the data breaches at Anthem, Premera, USIS, KeyPoint, and should have heightened awareness of federal agencies like OPM holding large sensitive data repositories.

Chapter 7: OPM's OCIO and its Federal Watchdog

Pursuant to the Inspector General (IG) Act of 1978, Inspectors General "provide a means for keeping the head of the establishment and the Congress fully and currently informed about problems and deficiencies relating to the administration of such programs and operations and the necessity for and progress of corrective action."[923] When President Carter signed the IG Act of 1978, he charged the IGs to always remember that their ultimate responsibility is not to any individual but to the public interest.[924]

The relationship between OPM's Office of the Inspector General (OIG) and its OCIO became strained while Katherine Archuleta served as Director and Donna Seymour as CIO. In fact, the relationship deteriorated to the point that IG Patrick McFarland took the drastic step of issuing a memorandum to Acting Director Beth Cobert to share "serious concerns" regarding the OCIO on July 22, 2015.[925]

The memorandum was issued just 12 days after Cobert was appointed Acting Director of the agency. During her nomination hearing before a Senate Committee,[926] Cobert was emphatic that she takes the relationship with the IG seriously, especially as it relates to enhancing cybersecurity.[927] Cobert met with the IG on her first day at OPM,[928] and she instituted regular meetings with the OIG thereafter.[929]

Despite serious concerns raised by the IG and Congress about Seymour's fitness to serve as CIO in the summer of 2015,[930] Cobert maintained support for Seymour and allowed her to remain on the job until her retirement on February 22, 2016.[931] The Committee obtained testimony in October 2015 that shows problems between the OCIO and the OIG persisted through the fall of 2015. An OIG employee testified that the relationship was strained, and the onus was on OIG staff to "chase down" information from the OCIO.[932]

---

[923] Inspector General Act of 1978 § 2; 5 U.S.C. app. § 2 (2012) (as amended).
[924] Council of the Inspectors Gen. on Integrity and Efficiency, *IG Act History* available: https://www.ignet.gov/content/ig-act-history.
[925] OIG Memo, *Serious Concerns*.
[926] *Nomination of the Honorable Beth F. Cobert to be Director, Office of Personnel Management: Hearing Before the S. Comm. on Homeland Sec. & Gov't. Affairs*, 114th Cong. (2016).
[927] *Id.*
[928] *Id.*
[929] *Incorporating Social Media into Federal Background Investigations: Hearing Before the Subcomm. on Gov't Operations and Subcomm. on Nat'l Sec.* of the *H. Comm. Oversight & Gov't Reform* 114th Cong. at 1:12.35 (2016).
[930] Letter from the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform, to the Hon. Beth Cobert, Interim Dir., U.S. Office of Pers. Mgmt (Aug. 6, 2015); *see also* Letter from 18 Members of Congress, to Barack Obama, President, United States (June 26, 2015) (raising concerns about OPM Director Katherine Archuleta and OPM Chief Information Officer Donna Seymour).
[931] Aaron Boyd, *OPM CIO Seymour Resigns Days Before Oversight Hearing*, FEDERAL TIMES (Feb. 22, 2016) available at: http://www.federaltimes.com/story/government/it/cio/2016/02/22/opm-cio-seymour-resigns/80766440/; Billy Mitchell, *Office of Personnel Management CIO Donna Seymour Retires*, FEDSCOOP, (Feb. 22, 2016) available at: http://fedscoop.com/opm-cio-seymour-retires; Ian Smith, *OPM CIO Donna Seymour Resigns*, FEDSMITH (Feb. 22, 2016) available at: http://www.fedsmith.com/2016/02/22/opm-cio-donna-seymour-resigns/.
[932] Special Agent Tr. at 46, 65-66.

Overall, however, the OCIO's relationship with the OIG steadily improved under Acting Director Cobert's leadership, and as of this report's publication, both offices report it to be without conflict.[933]

The IG's Memorandum of Concern

On July 22, 2015, the OPM IG wrote Acting Director Cobert to call attention to four situations where he felt the OCIO hindered his office's efforts, and five instances where he contended the OCIO provided incorrect and/or misleading information.[934]

MEMORANDUM FOR BETH F. COBERT
Acting Director

FROM: PATRICK E. McFARLAND
Inspector General

SUBJECT: Serious Concerns Regarding the Office of the Chief Information Officer

The memorandum stated:

> In certain situations, the OCIO's actions have hindered the OIG's ability to fulfill our responsibilities under the Inspector General Act of 1978, as amended (IG Act). Further, we have found that the OCIO has provided my office with inaccurate or misleading information, some of which was subsequently repeated by former OPM Director Katherine Archuleta at Congressional hearings.[935]

McFarland pointed out that the breakdown in the relationship stood in stark contrast to the relationship the OIG had with the OCIO in the past.[936] McFarland served as the agency's watchdog for twenty-six years.[937] Documents show the relationship between the OIG and OCIO did in fact deteriorate after being strong for years.

---

[933] *OPM Data Breaches: Part III: Hearing Before H. Comm. on Oversight & Gov't Reform*, 114th Cong. (Feb. 24, 2016) (prepared statement of Norbert E. Vint, Office of Inspector Gen., U.S. Office of Pers. Mgmt.) (hearing cancelled); *see also Incorporating Social Media into Federal Background Investigations: Hearing Before Subcomm. on Gov't Operations and Subcomm. on Nat'l Sec. of the H. Comm. on Oversight & Gov't Reform*, 114th Cong. at 1:12.35 (2016).

[934] U.S. Office of Pers. Mgmt. Office of Inspector Gen., Memorandum from Inspector Gen. Patrick McFarland to Acting Dir. Beth Cobert, Serious Concerns Regarding the Office of the Chief Information Officer (July 22, 2015) [hereinafter OIG Serious Concerns Regarding OCIO (July 22, 2015).]

[935] *Id.* at 1.

[936] *Id.*

[937] Carten Cordell, *OPM Inspector General Resigns, Leaving in February*, FED. TIMES, Feb. 3, 2016, http://www.federaltimes.com/story/government/management/agency/2016/02/03/opm-inspector-general-resigns-leaving-february/79756822/.

For example, in the April 2008 Semi-Annual Report to Congress, McFarland reported that then-Director Linda M. Springer had initiated a series of actions "to make sure that all OPM employees clearly understood what PII meant, the importance of protecting PII, and their responsibilities in protecting it."[938] The IG was to play an integral role in the efforts. The report stated:

> Director Springer requested that the OIG conduct an audit of one of OPM's largest program offices to ensure that they had developed and implemented effective controls over PII. . . . PII has also become a routine topic of discussion at the Agency's Information Technology Security Working Group meetings. The group was set up by the Chief Information Officer to ensure that information technology (IT) security and privacy policies, procedures and directives are communicated to all OPM program offices. On the technical side, OPM has made significant progress in implementing OMB requirements to safeguard PII.[939]



Former Inspector General Patrick McFarland testifies about data breaches

In 2015, however, McFarland had to resort to a public notification to Acting Director Cobert to call attention to the fact that his office was being undermined. McFarland wrote:

> In the past, the OIG has had a positive relationship with the OCIO. Although the OIG may have identified problems within the OCIO's areas of responsibility, we all recognized that we were on the same team, and the OCIO would leverage our findings in an effort to bring much needed attention and resources to OPM's information technology (IT) program.

---

[938] Office of Inspector Gen., U.S. Office of Pers. Mgmt., *Semiannual Report to Congress October 1, 2007 to March 31, 2008* (Mar. 2008), https://www.opm.gov/news/reports-publications/semi-annual-reports/sar38.pdf.
[939] *Id.*

> Unfortunately, this is no longer the case, and indeed, recent events make the OIG question whether the OCIO is acting in good faith.[940]

McFarland's memorandum was released to Congress and the public.[941] Chairman Chaffetz shared the IG's concerns. In a letter to Cobert, Chairman Chaffetz stated that he lost confidence in Seymour in the wake of the agency's announcement of the breaches, that his concerns were "amplified" by the IG's memorandum, and keeping Seymour in place only added "insult to injury" to those whose personal and sensitive information was stolen in the breaches.[942]

> On June 26, I communicated to President Obama that I have lost confidence in Ms. Seymour's ability to execute her role as CIO. 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. As a result, I asked the President to address this serious issue by removing Ms. Seymour from her position.
>
> I am deeply troubled Ms. Seymour remains at her post over a month after this request was made. My concerns about Ms. Seymour's ability to serve are amplified by a communication the Committee received from the Inspector General. In a letter dated August 3, 2015, OPM's IG notified me that on July 22, 2015 a memorandum was sent to you, and the letter advised me that "there have been situations where actions by the OCIO have interfered with, and thus hindered, the OIG's work. Further, the OCIO has repeatedly provided the OIG with inaccurate or misleading information."[1]

Excerpt from August 6, 2015 letter from Chairman Chaffetz to Acting Director Cobert

Cobert did not remove Seymour. In fact, Cobert gave Seymour a vote of confidence. *FedNewsRadio* reported:

> An OPM spokesman said by email that Cobert is pleased with Seymour and the entire CIO team's efforts to improve OPM's cybersecurity. . . . The [OPM] spokesman said Cobert responded to the IG's letter, saying 'In her first four weeks at OPM she has observed that the team, including the Office of the Chief Information Officer — working side-by-side with experts from across the federal government — has been working incredibly hard to enhance the security of our information technology systems and support those who have been affected by the recent cybersecurity incidents. The recent results of the Cybersecurity Sprint demonstrate the progress that has been made, although everyone recognizes there is more to do.'[943]

---

[940] OIG Serious Concerns Regarding OCIO (July 22, 2015) at 1.

[941] *Id.*

[942] Letter from the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform, to the Hon. Beth Cobert, Interim Dir., U.S. Office of Pers. Mgmt (Aug. 6, 2015).

[943] Jason Miller, *IG, Chaffetz Increase Heat on OPM CIO,* FEDNEWSRADIO, Aug. 6, 2015, available at: http://federalnewsradio.com/opm-cyber-breach/2015/08/ig-chaffetz-increase-heat-opm-cio/. The Cybersecurity Sprint was meant to increase the security of agencies systems. For additional information, *see* Exec. Office of the

Cobert said she was "committed to ensuring a cooperative relationship" between her teams and the OIG.[944] Cobert added that she "discussed the importance of the issue" with her leadership team and said they "are fully supportive of rebuilding a productive relationship, and fully understand how that will help us collectively deliver on OPM's mission."[945] The extremely serious nature of the concerns, however, raise questions about the decision to stand by Seymour.

Four Instances Where the OCIO Failed to Cooperate Fully

McFarland's letter to Cobert on July 22, 2015 identified four situations where the OCIO failed to cooperate with his office to the detriment of the agency.

Seymour failed to appropriately notify the IG of the April 2015 intrusion detection

In April 2015, the agency identified an unknown Secure Sockets Layer (SSL) certificate beaconing to a site (opmsecurity.org) that was not associated with OPM.[946] The agency reported this finding to US-CERT on April 15, 2015.[947] On Friday, April 17, 2015 at 11:39 a.m., OPM submitted several more questionable files to US-CERT,[948] and by 5:19 p.m. that evening, US-CERT confirmed the malicious nature of the executable files that OPM reported.[949]

The IG was not notified by OCIO—or anyone else at OPM—until one week later, on April 22, 2015.[950]

Under OPM's "Incident and Response and Reporting Guide," the OIG is an integral part of incident response.[951] For example, the Guide states that the OIG must be notified immediately if criminal activity is suspected.[952] The Guide instructs key OPM personnel to be trained in how to make notifications in a manner that serves the best interests of forensic investigations. It states that the OPM Computer Incident Readiness Team (OPM-CIRT) "must be trained in such areas as whom to contact when an incident occurs, how to preserve forensic evidence, and how

---

President, Press Release, *FACT SHEET: Enhancing and Strengthening the Federal Government's Cybersecurity* (June 12, 2015) https://www.whitehouse.gov/sites/default/files/omb/budget/fy2016/assets/fact_sheets/enhancing-strengthening-federal-government-cybersecurity.pdf.

[944] Memorandum from the Hon. Beth Cobert, Acting Dir., U.S. Office of Pers. Mgmt. to Patrick McFarland, Inspector Gen., U.S. Office of Pers. Mgmt., *Your Memo of July 22, 2015* (Aug. 3, 2015) [hereinafter Cobert Response to OIG Serious Concerns Regarding OCIO].

[945] *Id.*

[946] AAR Timeline – Unknown SSL Certificate (April 15, 2015) at HOGR020316-001922-1923 (OPM Production: April 29, 2016).

[947] *Id*; Email from [redacted] to CIRT (OPM) (April 15, 2015, 6:54 p.m.) at HOGR0724-000868 (OPM Production: Dec. 22, 2015).

[948] Email from [redacted] to Brendan Saulsbury, Senior Cyber Security Engineer, SRA (Apr. 17, 2015, 5:19 p.m.) at HOGR0724-000872- 75 (OPM Production: Dec. 22, 2015).

[949] *Id.*

[950] OIG Serious Concerns Regarding OCIO (July 22, 2015) at 3.

[951] U.S. Office of Pers. Mgmt., *Incident Response and Reporting Guide* at 3 (July 2009).

[952] *Id.* The Special Agent testified in October 2015 that this Guide was still the most current despite being dated July 2009. *See* Special Agent Tr. at 8.

to eradicate the various types of incidents. The training must also include when incidents are reported to US-CERT, the OPM IG, and appropriate law enforcement agencies."[953] The Guide states that "[c]omputer incidents are generally a lot easier to handle when reported promptly" and requires the Network Management Group Chief to help notify in a "timely manner" all "responsible parties," including the Assistant Inspector General for Investigations in the OIG.[954]

Documents and testimony show the OCIO failed to notify the OIG in a timely manner in April 2015. In fact, the IG found out about the breach by coincidence. The OIG Special Agent in Charge (SAC) ran into OCIO Director of IT Security Operations Jeff Wagner in the hallway. Wagner asked the SAC to meet later in the day (at which time the SAC was informed of the first breach)."[955]

The SAC, noticed Wagner on the sixth floor of OPM around lunch time, which was unusual because Wagner worked on a different floor. The SAC testified:

> As I recall it, it was truly a chance encounter. I was exiting from the elevator on the sixth floor. I was walking down the hallway. Jeff Wagner and a coworker -- I don't recall who the coworker was or to this day don't remember -- was walking into the Federal Investigative Service Office, which is in the hallway of the sixth floor, and as I was approaching Jeff, waved, nodded, as I know who Jeff is. And Jeff said: Hey, when [you] get a chance, come down to my office. And we -- or I continued on into my office.[956]

The SAC testified that the entire conversation lasted no longer than thirty seconds, and that "I would describe this as a conversation in passing. Literally, he was walking into an office; I was walking towards my office."[957]

The SAC testified to not knowing what Wagner wanted to discuss at the meeting Wagner requested.[958] In fact, the SAC thought Wagner may have wanted to discuss Federal Employee Health Benefits (FEHB) program carriers. The SAC stated:

> So I immediately went back to my office, and as I recall, I thought this was in reference to another potential breach. We had the Anthem breach earlier, I believe February 2015. March of 2015, you had the Premera. Those were large FEHBP carriers. We were still trying to sort out what the impact to not only FEHBP subscribers but the FEHBP as a whole and its financial integrity. I immediately thought this was another breach of a FEHBP carrier when I left Jeff.[959]

---

[953] U.S. Office of Pers. Mgmt., *Incident Response and Reporting Guide* at 12.
[954] *Id.*
[955] OIG Serious Concerns Regarding OCIO (July 22, 2015) at 3.
[956] Special Agent Tr. at 11.
[957] *Id* at 12.
[958] *Id.*
[959] *Id.* at 12-13.

When the SAC visited Wagner later that afternoon, the SAC learned OPM had suffered an intrusion. Wagner handed the SAC a security incident timeline that included a series of dates and bullets.[960] The earliest date was April 15, 2015, and there was an attached description that stated: "Zero day, malicious activity found."[961] The SAC testified: "what immediately jumped out to me was internal notifications were made. The FBI was called. Also the United States Department of Homeland Security, US-CERT team, the Computer Emergency Response Team, had been called and notified."[962]

The SAC recalled being "shocked" that law enforcement was in the building and that the OIG was unaware.[963] With respect to why it was important for the OIG to receive timely notice, the SAC stated:

> A. There are several reasons why. First, the IG Act. It's the agency's responsibility to notify the IG of potential incidents or situations that impact the agency so the IG can timely -- or do its job in a timely matter of notifying Congress.
>
> You have the FISMA Act, which is the Federal Information Management Security Act, which requires notification of the appropriate IG, of what I recall of a potential -- or what I recall and believe it states of a potential situation -- we would be the appropriate IG in that situation -- and by their own incident and reporting guide of 2009.
>
> The other thing is just basically common courtesy. I would expect Jeff's office -- especially if you have people walking into the building with guns. I'm also responsible if there is an active shooter in the building of deploying assets, and it can obviously be a very terrible situation if we don't realize what other people are in the building that are armed at that particular time.
>
> Q. So you're saying if other law enforcement officers were in the building --
>
> A. Sure.
>
> Q. you would be the one responsible for coordinating with those individuals?
>
> A. Correct.[964]

---

[960] *Id.* at 13-14
[961] *Id.*
[962] *Id.* at 14.
[963] *Id.* at 16.
[964] *Id.* at 15-16.

The SAC testified that Wagner said OPM had no intention of notifying the public, and that the OIG disagreed with that plan.[965] The SAC testified that Wagner said "there was no need" to notify the public, and that Wagner believed there was "no evidence" the agency had lost information to the attackers, and that the situation was being carefully monitored.[966] **By April 22, 2015, however, OPM already found evidence of a serious breach**. OPM eventually announced that it lost the personnel records of 4.2 million federal employees on June 4, 2015.[967]

The failure of the OCIO to notify the IG in a timely manner undermines the important role Congress has established for the IGs. Like all federal watchdogs, McFarland's ultimate responsibility during this time was not to any individual, but to the public interest.[968] Being prevented from taking part in the investigation into the cyber intrusion from day one hampered the IG's ability to effectively carry out its work on behalf of the public, and also undermined the public's trust that the agency was acting in good faith. As conveyed by McFarland, "Failure to include OIG investigators and auditors from the beginning of the incident impeded our ability to coordinate with other law enforcement organizations and conduct audit oversight activity."[969]

Seymour failed to notify the OIG of the loss of background investigation data in a timely manner

With respect to the loss of background investigation materials, the Special Agent testified that the OIG was notified unintentionally. The SAC testified:

> So, it was another right place at the right time type of situation. On or about May 18, 2015, I had received information that there was another breach at an FEHBP carrier, this time being CareFirst. CareFirst is an extremely large FEHBP carrier, and this caused us great concern. I called Jeff [Wagner] on or about May 18th, May 19th, that evening, asking if he had heard anything about the CareFirst situation.[970]

The SAC stated that Wagner had not heard anything about CareFirst, and they agreed to continue checking-in with each other.[971] Two days later, on May 20, 2015, the SAC saw news about a breach at CareFirst and tried to contact Wagner "several times that day."[972] The Special Agent recounted watching the news and deciding to call Wagner. The SAC stated:

> A. It was -- as I recall, it was approximately 6 to 6:30 that night before I was leaving for the day. I called Jeff. Jeff picks up the phone. I was -- almost jumped through the phone, as I recall,

[965] *Id.* at 17-18.
[966] *Id.*
[967] U.S. Office of Pers. Mgmt., Press Release, *OPM to Notify Employees of Cybersecurity Incident* (June 4, 2015), available at: https://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident/.
[968] Council of the Inspectors Gen. on Integrity and Efficiency, *IG Act History*, available at: https://www.ignet.gov/content/ig-act-history (last visited June 4, 2016).
[969] OIG Serious Concerns Regarding OCIO (July 22, 2015) at 3.
[970] Special Agent Tr. at 19.
[971] *Id.*
[972] *Id.* at 19-20.

saying: Jeff, have you heard anything about CareFirst? And Jeff's initial response was: Where are you? And I said: I'm still up in the office. And Jeff said: I need to come see you. So I met him at the door. It was only a few minutes. Jeff was obviously in the building. It was a few minutes. He came up. I escorted him into the conference room. Jeff sat down. And the best way to describe it was, it was totally different than the April meeting that had occurred. I knew something was up just by his body language, and sat down. And Jeff initially said: They got it. I looked at him, and he then repeated: They got all of it. And I asked the question: CareFirst? And he was like, no. I said something to the effect of: How big is this? And as I recall, Jeff said: Homeland Security or US-CERT is down here. FBI is down here. We had a couple of questions, but Jeff just didn't have a lot of information. It was truly different than the April meeting; whereas, you know, we were asking questions, Jeff seemed to be able to respond, this one was certainly not that way.

Q. And did he specifically at this time indicate that background investigation records may have been compromised?

A. He speculated that, yes, they had. But we were -- I was also asking about other systems that are controlled by the Office of Personnel Management, but, yes, Jeff did speculate that background investigations, the SF-86s.[973]

The SAC testified that the scene on May 20, 2015 was dismal, and that it "looked like somebody was defeated. I mean, this was a man who was defeated. The shoulders were slouched, and it had obviously been a -- my recollection, from what I recall, I would classify as a long day."[974]

The SAC accompanied Wagner to meet personnel from the FBI and US-CERT. The Special Agent testified that Wagner said law enforcement personnel were on site, and that Wagner willingly introduced the SAC to the law enforcement officials on site.[975]

Later that day, when the SAC reported the news to OIG colleagues, **nobody was aware of the cyber investigation that was underway just a few floors below**.[976] The SAC stated that after the April 22, 2015 discussion with Wagner, until the May 20, 2015 conversation in the OIG's conference room about the loss of background investigation material, the two had "no substantial conversations."[977] The SAC stated:

---

[973] *Id.* at 20-21.
[974] *Id.* at 45 (emphasis added).
[975] *Id.* at 21.
[976] *Id.* at 22.
[977] *Id.*at 45.

It was just more work was going on in reference to that. Our conversations primarily focused on, again, the FEHBP carriers and finding out more information about the Anthem breach, finding more information about Premera breach, working with the FBI and what information they needed.[978]

Seymour failed to notify the OIG about the 2014 incident

The IG's notification to Acting Director Cobert did not follow an isolated incident, but rather a series of incidents where it was not notified immediately or promptly by the OCIO. In addition to failing to promptly notify the OIG about the breaches in April 2015 and May 2015, the SAC also testified that the OCIO failed to provide timely notification concerning a breach that US-CERT identified on March 20, 2014 at OPM. The SAC stated:

> Q. Okay. Would you characterize the IG's notification of this March 2014 incident as being timely?
>
> A. No.
>
> Q. Would you characterize it as being in keeping with OPM policy and rules governing notification to the OIG?
>
> A. No.
>
> Q. Today we have discussed three separate cybersecurity incidents occurring at OPM since March 2014. From your perspective, having been involved with all three events, how would you characterize OPM's notification to the Office of Inspector General for these three incidents?
>
> A. I would characterize it as nonexistent. There was -- my opinion -- there was no formal notification to any of these incidents. It was -- the first one, the March 2014, we were notified by another agency; the April 2015, I was just getting off the elevator and happened to be there; and then the May 2015, I proactively reached out to the agency in reference to another issue, and that's how we were notified."[979]

In summary, when McFarland wrote Cobert to raise concerns about the OCIO's failures to notify his office in a timely manner about major cybersecurity events, as the IG Act, FISMA, and OPM's own guidance direct, the IG could have cited even more examples. The OCIO's repeated failure to involve the OIG eroded the relationship between the two offices and prevented the OIG from conducting its important work on behalf of the American public.

---

[978] *Id.* at 43-44.
[979] *Id.* at 26-27.

Meetings with Federal Law Enforcement Agencies

Under OPM's "Incident Response and Reporting Guide," the OIG is "responsible for providing law enforcement authority and investigative support to any incident handling initiatives."[980] The Guide makes clear that the OIG must be notified immediately if criminal activity is suspected, and that "As determined by the OIG, other law enforcement support may be called in to assist in the investigation of an incident."[981]

While the guide clearly states the OIG should be an integral part of any law enforcement activity and determine the need for law enforcement support, the OIG was not even consulted about the need to bring in law enforcement support for this particular incident response. In fact, the OIG was prevented from even attending key meetings with other federal law enforcement agencies. McFarland raised these concerns to Cobert. He wrote:

> During the investigation of the second breach involving background investigation files, the OIG requested to attend meetings between OCIO staff, the Federal Bureau of Investigations (FBI), and the DHS U.S. Computer Emergency Readiness Team (US-CERT). Former Director Archuleta stated that the OIG could not attend these meetings because our presence would 'interfere' with the FBI and US-CERT's work.[982]
>
> * * *
>
> This action is a violation of the Inspector General Act of 1978, as amended (IG Act). The OIG contacted the FBI and US-CERT directly and did indeed meet with them without adversely affecting the progress of the investigation. These meetings provided the OIG with critical information necessary for our own investigatory and audit work. What the former Director considered 'interference' was simply the OIG fulfilling our responsibilities.[983]

The SAC told the Committee that on May 20, 2015, after Wagner relayed that "they got all of it,"[984] the SAC asked Wagner: "Can I go down and meet [law enforcement personnel]?"[985]

The SAC testified: "I immediately asked, because I did not meet the investigators from the previous breach. I wanted to go down, introduce myself, and meet the investigators."[986] Wagner responded, "Absolutely, no problem," and escorted the SAC to a room where "a large number of investigators" were sitting and that "most had been sitting there and had their laptops

---

[980] U.S. Office of Pers. Mgmt., *Incident Response and Reporting Guide* at 3.
[981] *Id.*
[982] OIG Serious Concerns Regarding OCIO (July 22, 2015) at 3.
[983] *Id.* at 3-4.
[984] Special Agent Tr. at 20.
[985] *Id.* at 46.
[986] *Id.*.

up and running."[987] The SAC testified that Wagner introduced him to the law enforcement officials.[988] The SAC offered assistance, and left.[989]

The following day, on May 21, 2015, OPM Director Katherine Archuleta requested a meeting with IG McFarland in the situation room, a small room where classified briefings can occur.[990] McFarland and his Deputy, Norbert ("Bert") Vint, attended the meeting with Archuleta, and they debriefed OIG staff immediately afterwards.[991] The SAC testified that Vint recalled "the Director asked IG McFarland to stop interfering with the investigation."[992] The SAC stated:

> My personal recollection, as I recall, I was stunned at this because the investigator that they were talking about was me. I was there that night receiving the notification from Jeff. I reiterated to both Pat [McFarland] and Bert [Vint] that the May 20th date, I was trying to get ahold of Jeff. There were several times that day I reached out to Jeff; I emailed Jeff; I called Jeff. It was not in reference to this. I had no idea this was going on. Again, I was under the impression that [Wagner] was working the CareFirst breach and [I] wanted more -- desperately wanted more information about this.[993]
>
> * * *
>
> I have never had a situation where the agency has -- I perceived -- as I recall, I perceived it, as the former Director Archuleta was telling Pat [McFarland] that he had a heavy-handed agent who was going down there demanding information. And as I recall, there could be nothing further from the truth. That's why it stands out in my mind. This is such an outlier of anything or any feedback that has ever come from our office. And I recognize there are situations where agencies and IGs may not agree, but to the point where there was a complaint that asserted we were interfering, no, I was just stunned by that.[994]

KeyPoint Audit

Documents and testimony show the OCIO also interfered with the IG's audits. McFarland wrote:

> In October 2014, due to concerns raised after a security breach at United States Investigative Services (USIS) was identified in June 2014, the U.S.

---

[987] *Id.* at 47.
[988] *Id.* at 46-47.
[989] *Id.*.
[990] *Id.* at 23.
[991] *Id.*
[992] *Id.* at 24.
[993] *Id.*
[994] *Id.* at 25.

> Office of Personnel Management (OPM) Office of the Inspector General (OIG) informed the OPM Chief Information Officer (CIO) of our intent to audit KeyPoint Government Solutions (KeyPoint).
>
> At an October 16, 2014 meeting, the CIO requested that we delay this audit, stating that the U.S. Department of Homeland Security (DHS) had just completed a comprehensive assessment of KeyPoint, which was also in response to the USIS breach. Therefore, she was concerned that our audit would interfere with KeyPoint's remediation activity.
>
> The OIG tries to coordinate our oversight work with the OPM program offices to the maximum extent possible, and so we agreed to delay our audit. We later discovered, however, that OPM became aware in early September 2014 that KeyPoint had been breached. Despite knowing this, the CIO did not inform OIG staff of the breach in the October 16th meeting when she requested that we delay our audit work.[995]
>
> * * *
>
> Our audit, which was a comprehensive evaluation of the information technology (IT) security posture of Key Point, was delayed for over three months. The DHS review was focused on incident response objectives, and did not have as wide of a scope as the CIO alluded. In fact, our audit identified a variety of areas that were not part of DHS's review where KeyPoint could improve its IT security controls. The CIO's interference with our audit agenda resulted in additional time passing with these vulnerabilities still present in KeyPoint's environment. The delay also prevented us from communicating important information that may have been relevant to the recent Congressional hearings regarding the OPM data breaches."[996]

This situation is significant and a concern because the OIG has a track record of conducting valuable work related to OPM's security posture. There is no basis—legal or otherwise—for OPM officials to delay or otherwise interfere with the IG's work.

Notification Concerning New IT Infrastructure

The IG alleged the OCIO prevented the IG from being involved in the development of its new IT infrastructure from the start. After a March 2014 cyber incident,[997] OPM/OCIO launched a project to overhaul OPM's IT infrastructure. This project involved a multi-phase approach, including: Tactical (improving the existing security environment), Shell (creating a new data center and IT architecture), Migration (migrating all OPM systems to the new

[995] OIG Serious Concerns Regarding OCIO (July 22, 2015) at 3.
[996] *Id.*
[997] OIG Flash Audit Alert (June 17, 2015) at 5.

architecture), and Cleanup (decommissioning existing hardware and systems).[998] The agency awarded a sole source contract for this multi-phased project, and the contract was initially managed by CIO Seymour.[999]

The IG stated that the OCIO, again, failed to work in good faith with the OIG on this initiative. McFarland wrote:

> The OCIO failed to inform the OIG of a major new initiative to overhaul the agency's IT environment. We did not learn the full scope of the project until March 2015, nearly a year after the agency began planning and implementing the project. This exclusion from a major agency initiative stands in stark contrast to OPM's history of cooperation with our office.[1000]

The IG found out about the IT Infrastructure Improvement project on March 2, 2015, when the Deputy IG met with the OCIO Chief of Staff regarding a special funding request.[1001] Specifically, the IG learned for the first time at this meeting that he was "expected to pay the agency approximately $1.16 million in FY2015 funds" to support the project.[1002] The OCIO Chief of Staff told the Deputy IG that this would be a one-time assessment, but then later was told the assessments would be annual.[1003]

The IT Infrastructure Improvement project implicated a significant amount of money. In late October 2015, OPM advised the Committee that it had spent approximately $60 million in FY2014 and 2015 on the project.[1004] About eighty percent of the funds originated from OPM's revolving fund and the remaining twenty percent from a variety of discretionary and mandatory funds areas.[1005]

According to McFarland, despite the high stakes of the project for IT security, delivery, and costs, the OCIO excluded the OIG. McFarland wrote:

> The role of the OIG is to promote economy, efficiency, and effectiveness in the administration of the agency's programs, as well as to keep the Director, Congress, and the public informed of major problems and deficiencies. Because the OIG was not involved, agency officials were denied the benefit of an independent and objective evaluation of the

---

[998] *Id.*

[999] Imperatis Letter Contract (June 16, 2014), Attach. 1 at 000002 (Imperatis Production: Sept. 1, 2015); *id.* Attach. 1 at 000011. A sole source contract is a contract that was awarded without being subject to the competitive bidding process.

[1000] OIG Serious Concerns Regarding OCIO (July 22, 2015) at 4.

[1001] U.S. Office of Pers. Mgmt., "Background Information: OPM Infrastructure Overhaul and Migration Project" (June 17, 2015) (on file with the Committee).

[1002] *Id.*

[1003] *Id.*

[1004] Email from U.S. Off. of Pers. Mgmt. to H. Comm. on Oversight & Gov't Reform Staff (Oct. 28, 2015) (on file with the Committee).

[1005] *Id.* (OPM requested $21 million in FY2016 to implement and sustain these improvements. The FY2016 omnibus requires OPM to use $21 million of its $272 million appropriated dollars for IT security improvements).

> project's progress from the beginning. The audit work that we have performed since learning of this project has identified serious deficiencies and flaws that would have been much easier to address had we been able to issue recommendations earlier in the project's lifecycle.[1006]

The OCIO's decision to exclude the IG hurt the agency because it lacked information that could have informed the decision-making and planning stages for the IT infrastructure overhaul. The project was exposed to waste, fraud, and abuse partly because of the OCIO's posture with respect to involving the OIG.

Five Incorrect and/or Misleading Statements

McFarland's July 22, 2015 Memorandum cited five incorrect and/or misleading statements to Congress. In the public version of the memorandum, the descriptions of those five incorrect and/or misleading statements were fully redacted.

First Misstatement before the Senate Committee on Appropriations

At a hearing before a Senate Committee on Appropriations' Subcommittee on Financial Servcies and General Government, former Director Katherine Archuleta stated that OPM completed a Major IT Business Case (formerly known as the OMB "Exhibit 300") for the infrastructure improvement project.[1007] McFarland also wrote that "OPM indicated [in response to the flash audit] that they have been in 'continual consultation and discussion with OMB [the Office of Management and Budget]' regarding this project."[1008] According to McFarland, however:

> OPM has not completed a Major IT Business Case, and has not provided us with any evidence that it has consulted with OMB regarding the full scope of the project and that OMB approved OPM's approach. In its June 22nd response to the flash audit alert OPM acknowledged that it has not completed this document (and actually disagrees with our recommendation to prepare one). After the hearing, the OIG again requested documentation supporting OPM's statements, and again the agency has failed to produce any evidence whatsoever that it has kept OMB apprised of the full scope and scale of this project.[1009]

[1006] OIG Serious Concerns Regarding OCIO (July 22, 2015) at 4.
[1007] *OPM Information Technology Spending and Data Security: Hearing Before Subcomm. on Financial Services & Gen. Gov't of the S. Comm. on Appropriations* 114th Cong. at 1:40 (June 23, 2015) [hereinafter *Hearing on OPM Information Technology Spending and Data Security*].
[1008] OIG Serious Concerns Regarding OCIO (July 22, 2015) at 5.
[1009] *Id.*

Second Misstatement Before the Senate Committee on Appropriations

Former Director Archuleta testified at a June 23, 2015 Senate subcommittee hearing that "my CIO has told me that we have, indeed, an inventory of systems and data."[1010] According to McFarland, however:

> Both our flash audit alert and Fiscal Year (FY) 2014 FISMA audit noted that OPM does not maintain a comprehensive inventory of its information technology (IT) assets. We confirmed with the Chief Information Officer (CIO) on June 23, 2015, and again with her staff on June 29th, that OPM is still in the process of developing a comprehensive information system inventory and this process is not yet complete.[1011]

Third Misstatement Before Senate Committee on Appropriations and House Committee on Oversight and Government Reform

Archuleta and Seymour testified before the Senate Appropriations Committee and the House Committee on Oversight and Government Reform that the sole-source contract with Imperatis only covered the first two phases of the IT Infrastructure Improvement project, and that contracts for the migration and cleanup phases of the project had not yet been awarded.[1012] According to McFarland, however:

> The document that justified the sole-source contract clearly stated that it was intended to be used for the full scope of the project, and that full and open competition would be pursued if and when it became appropriate to do so. Further, the statement of work contained in the contract itself specifically states that '[t]he Contractor shall complete the work within this [statement of work] in four different phases: Tactical, Shell, Migration, and Clean Up.' When OIG personnel met with the OCIO on May 26, 2015, to discuss concerns regarding the use of a sole-source contract for all phases of the project, the CIO argued strongly in favor of this approach. She informed us that she wanted the same contractor to oversee all four phases of the project for continuity purposes.[1013]

[1010] *Hearing on OPM Information Technology Spending and Data Security* at 1:40.
[1011] OIG Serious Concerns Regarding OCIO (July 22, 2015) at 5.
[1012] *Hearing on OPM Information Technology Spending and Data Security* at 2:14 (former OPM Director Archuleta: "I would like to remind the Inspector General that contracts for the Migration and Cleanup have not yet been awarded."); *Hearing on OPM Data Breach: Part II* at 2:10.00 (former OPM Director Archuleta: "I would like to remind [the IG] that the contracts for Migration and Cleanup have not yet been awarded. And we will consult with him as we do that."); *id.* at 2:58.00 (CIO Seymour: " ... that's why we only contracted for the first two pieces and we said as we work through this project to understand it, we'll be able to better estimate and understand what needs to move into that Shell.").
[1013] OIG Serious Concerns Regarding OCIO (July 22, 2015) at 6.

Fourth Misstatement Before the House Committee on Oversight and Government Reform

During a hearing before the Committee on Oversight and Government Reform, in response to a question about the eleven systems operating without a valid Security Assessment and Authorization (Authorization) as of the end of FY 2014, Seymour stated this was no longer a concern because she had granted an interim Authorization to these systems.[1014] According to McFarland, however, OMB does not allow interim or extended Authorizations.[1015] Therefore, the CIO's "extension," from the IG's perspective, was not valid, and the eleven systems identified in the 2014 audit have still not been subject to the Authorization process.[1016]

Fifth Misstatement Before the Senate

At a June 25, 2015 Senate hearing, former Director Archuleta stated that OPM had received a special exemption from OMB related to system Authorization because of the ongoing infrastructure improvements.[1017] Office of Management and Budget CIO Tony Scott was unable to confirm this during the hearing.[1018] After the hearing, however, the IG found OMB submitted a request to OPM for evidence supporting this claim. According to McFarland, OPM officials responded by telling OMB that Archuleta did not make such a statement. McFarland found: "This is incorrect, as the statement can be found at timestamp 1:47 of the hearing."[1019]

The agency disagreed with McFarland with respect to the truthfulness of these statements to Congress. The IG's allegations, however, are very serious, and they are supported by documents and other evidence. Providing false testimony to Congress is a crime and these statements should be evaluated by the Department of Justice to determine whether a prosecution may be justified.

Current State of Relationship

McFarland wrote to Cobert: "It is imperative that these concerns be addressed if OPM is to overcome the unprecedented challenges facing it today."[1020] Indeed, OPM has taken actions to improve communication with the OIG. Following the July 2015 memorandum, Cobert

---

[1014] *OPM Data Breach: Hearing Before H. Comm. on Oversight & Gov't Reform*, 114th Cong. at 2:27.00 (June 16, 2015), available at: https: //oversight.house.gov/hearing/opm-data-breach/ (form OPM CIO Donna K. Seymour: "Sir, I have extended the Authorizations that we had on these systems because we put a number of security controls in place in the environment."). *See also Hearing on OPM Information Technology Spending and Data Security* at 1:36 (former Director Archuleta: "I can tell you that all but one of those systems has been Authorized."); *Hearing on OPM Data Breach: Part II* (statement of former Director Archuleta) ("Of the systems raised in the 2014 audit, 11 of those systems were expired. One of those, a contractor system, is presently expired. All other systems raised in the [2014] audit have either been extended or provided a limited Authorization.").

[1015] OIG Serious Concerns Regarding OCIO (July 22, 2015) at 6.

[1016] *Id.*

[1017] *Id.* at 7.

[1018] *Id.*

[1019] *Id.*

[1020] *Id.* at 1.

instituted regular meetings between the OCIO and OIG to cover key issues, such as planning and new projects.[1021]

> 1) In addition to the bi-weekly meetings we have recently established between you and I (IG-Director Meetings), and the weekly meetings we have recently established between your senior staff and mine (Senior Staff Meetings), we believe we would also both benefit from separate, regularly scheduled meetings between your IT team and OCIO (IG-OCIO Meetings). We propose, at the outset, that we would meet once a month, and can adjust the frequency as needed. We would propose leadership involvement in those meetings, whenever possible, as well. Our OCIO team will come prepared to brief you on recent events and progress on ongoing activities, and you will have the opportunity to raise any questions or concerns on a regular basis. Typical agenda items would include, but not be limited to:
>
> a. Short term and long-term planning;
> b. Proposed new projects;
> c. Updates on ongoing projects, gaps in deliverables, and plans to address any such gaps;
> d. Identification and mitigation of any technical issues that might develop;
> e. FISMA audits and compliance.

OIG Memo, Serious Concerns (July 2015)

In testimony prepared for a February 2016 Committee hearing that was canceled following the resignation of OPM CIO Donna Seymour two days prior, Acting Inspector General Norbert E. Vint stated:

> The productivity of those meetings has improved over time, and through these meetings, we have been able to work through certain issues. The OCIO has also begun to consult with us more often, such as when they instituted the recent '[Authority to Operate] Sprint.'[1022]

Vint stated the relationship improved under Cobert, and that there were no further problems with respect to accessing information.[1023] Vint was prepared to testify that, "Consequently, we have no reason to believe that they have intentionally provided us with inaccurate information or withheld material facts."[1024]

[1021] *Id.*
[1022] *OPM Data Breaches: Part III: Hearing Before H. Comm. on Oversight & Gov't Reform*, 114th Cong. (Feb. 24, 2016) (prepared statement of Norbert E. Vint, Office of Inspector Gen., U.S. Office of Pers. Mgmt.) (hearing cancelled).
[1023] *Id.*
[1024] *Id.*



Cobert testifies about the agency's relationship with the Inspector General before the Committee on May 13, 2016

It is also noteworthy that Cobert added cyber talent to the agency.[1025] McFarland attributed improvement in the OCIO-OIG relationship to one of these staff additions.[1026] On November 4, 2015, Cobert announced the addition of Clifton ("Clif") Triplett to the OPM cyber team.[1027] Reporting directly to Cobert, Triplett is tasked with advancing the state of enterprise architecture and cybersecurity, including information technology investments, capabilities, and services.[1028] Working alongside OPM's CIO—currently Acting CIO Lisa Schlosser[1029]—Triplett supports the ongoing response to the 2015 incidents, completing the development of OPM's plan to mitigate future incidents, and recommends further improvements to best secure OPM's IT architecture.[1030] Triplett has thirty years of broad executive management experience, including work on Top Secret and other advanced technologies in the protection and defense of the U.S. Nuclear Command and Control Systems.[1031]

Vint's draft testimony stated that Triplett helped to mend internal relationships. Vint's testimony stated:

> We believe that the new Senior Cyber and Information Technology Advisor, Clifton N. Triplett, has helped facilitate this improved

---

[1025] U.S. Office of Pers. Mgmt., Press Release, *OPM Director Announces Key New Cyber Advisor* (Nov. 4, 2015), https://www.opm.gov/news/releases/2015/11/opm-director-announces-key-new-cyber-advisor-2/.
[1026] *OPM Data Breaches: Part III: Hearing Before H. Comm. on Oversight & Gov't Reform*, 114th Cong. (Feb. 24, 2016) (prepared statement of Norbert E. Vint, Office of Inspector Gen., U.S. Office of Pers. Mgmt. at 5) (hearing cancelled).
[1027] U.S. Office of Pers. Mgmt., Press Release, *OPM Director Announces Key New Cyber Advisor* (Nov. 4, 2015), https://www.opm.gov/news/releases/2015/11/opm-director-announces-key-new-cyber-advisor-2/.
[1028] *Id.*
[1029] U.S. Office of Pers. Mgmt., *Lisa Schlosser: Acting Chief Information Officer* (May 17, 2016), https://www.opm.gov/about-us/our-people-organization/senior-staff-bios/lisa-schlosser/.
[1030] U.S. Office of Pers. Mgmt., Press Release, *OPM Director Announces Key New Cyber Advisor* (Nov. 4, 2015), https://www.opm.gov/news/releases/2015/11/opm-director-announces-key-new-cyber-advisor-2/.
[1031] *Id.*

> relationship as well as create additional avenues of communication between the OIG and the agency's IT staff. It appears that Triplett's role is to provide high level advice to assist the Acting Director in developing a strategy to address the multitude of IT challenges facing OPM. I and other senior OIG officials meet with Triplett on almost a weekly basis. From what we understand, he agrees with the OIG that the agency needs to have a comprehensive plan moving forward that would include a short-term plan to address the needs of OPM's critical IT systems, as well as a long-term plan for the implementation of OPM's agency-wide Infrastructure Improvement Project."[1032]

Cobert testified that the relationship had improved from her perspective. In response to a question from Rep. Mark Meadows (R-NC) at a hearing on May 13, 2016, Cobert testified:

> We have been working across the agency to strengthen our effectiveness of our dialogue with the CIO and I believe we've made real progress in a number of different areas. We've set up a cadence of regular communications at my level with the Inspector General, currently Acting Inspector General. On a bi-weekly basis, we meet and get an overview of the issues. We have specific working teams that meet on a periodic basis as well - both around the CIO, around procurement, we've set up that same kind of mechanism on the stand-up of the NBIB given the oversight issues there and wanting to make sure we get those right. So I think we've made considerable progress in terms of the dialogue, the clarity of the communications. We welcome their input on what we could be doing as better. As we welcome input from our colleagues here and elsewhere."[1033]

Cobert characterized the relationship as "much improved."[1034] While the OIG reported being "pleased" that communications have improved, the office was "still concerned about OPM's overall IT strategy."[1035] Vint committed that the OIG would "continue to monitor the OCIO's activities and work with them to ensure that actions discussed at meetings are, in fact, implemented – and implemented in accordance with proposed timelines."[1036]

[1032] *OPM Data Breaches: Part III: Hearing Before H. Comm. on Oversight & Gov't Reform*, 114th Cong. (Feb. 24, 2016) (prepared statement of Norbert E. Vint, Office of Inspector Gen., U.S. Office of Pers. Mgmt.at 5) (hearing cancelled).

[1033] Incorporating Social Media into Federal Background Investigations: Hearing Before Subcomm. on Gov't Operations and Subcomm. on Nat'l Sec. of the H. Comm. on Oversight & Government Reform, 114th Cong. at 1:12.35 (May 13, 2016), https://oversight.house.gov/hearing/incorporating-social-media-federal-background-investigations/.

[1034] *OPM Data Breaches: Part III: Hearing Before H. Comm. on Oversight & Gov't Reform*, 114th Cong. (Feb. 24, 2016) (prepared statement of Norbert E. Vint, Office of Inspector Gen., U.S. Office of Pers. Mgmt.at 5) (hearing cancelled).

[1035] *Id.*

[1036] *OPM Data Breaches: Part III Hearing Before H. Comm. on Oversight & Gov't Reform*, 114th Cong. (Feb. 24, 2016) (prepared statement of Norbert E. Vint, Office of Inspector Gen., U.S. Office of Pers. Mgmt. at 5) (hearing cancelled).

Summary of OIG and OCIO relationship

Federal watchdogs play a critical role in the federal government, one that is statutorily-driven by the Inspector General Act of 1978. Despite the key role IGs play, the relationship between OPM OIG and its OCIO became strained while Katherine Archuleta served as Director and Donna Seymour as CIO. Despite serious concerns raised by the OIG in July 2015, and despite concerns raised by Congress about Seymour,[1037] Acting Director Cobert maintained support for Seymour, allowing her to hold a leadership role until her retirement on February 22, 2016.[1038] Overall however, the OCIO's relationship with the IG steadily improved under Acting Director Cobert's leadership and today is reported by both entities to be without conflict.[1039] The future effectiveness of the agency's information technology and security efforts will depend on a strong relationship between these two entities moving forward.

[1037] Letter from the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform, to the Hon. Beth Cobert, Interim Dir., Office of Pers. Mgmt (Aug. 6, 2015); Letter from 18 Members of Congress, to Barack Obama, President, United States (June 26, 2015) (raising concerns about OPM Director Katherine Archuleta and OPM Chief Information Officer Donna Seymour).

[1038] Aaron Boyd, *OPM CIO Seymour Resigns Days Before Oversight Hearing*, FEDERAL TIMES, Feb. 22, 2016, *available at:* http://www.federaltimes.com/story/government/it/cio/2016/02/22/opm-cio-seymour-resigns/80766440/; Billy Mitchell, *Office of Personnel Management CIO Donna Seymour Retires*, FEDSCOOP, Feb. 22, 2016, available at: http://fedscoop.com/opm-cio-seymour-retires; Ian Smith, *OPM CIO Donna Seymour Resigns*, FEDSMITH, Feb. 22, 2016, available at: http://www.fedsmith.com/2016/02/22/opm-cio-donna-seymour-resigns/.

[1039] *OPM Data Breaches: Part III: Hearing Before H. Comm. on Oversight & Gov't Reform*, 114th Cong. (Feb. 24, 2016) (prepared statement of Norbert E. Vint, Office of Inspector Gen., U.S. Office of Pers. Mgmt.at 5) (hearing cancelled); *Incorporating Social Media into Federal Background Investigations: Hearing Before Subcomm. on Gov't Operations and Subcomm. on Nat'l Sec. of the H. Comm. on Oversight & Gov't Reform*, 114th Cong. (May 13, 2016).

Chapter 8: The IT Infrastructure Improvement Project: Key Weaknesses in OPM's Contracting Approach

On March 20, 2014, DHS/USCERT informed OPM that a third party had exfiltrated data from OPM's network.[1040] In response to this discovery and after identifying serious vulnerabilities in the OPM network, the agency initiated the IT Infrastructure Improvement project. Seymour testified before the Committee that this project began as a consequence of the March 2014 cyber incident.[1041]

This project was intended to quickly secure OPM's legacy IT environment with the urgent procurement of security tools (Tactical, phase 1) and to fully overhaul OPM's IT infrastructure with a new IT environment that included security controls (building the Shell, phase 2). After building the new IT environment (the Shell), the plan was to migrate OPM's entire IT infrastructure into the new IT environment (Migration, phase 3) and then decommission legacy IT hardware and systems (Clean Up, phase 4). In June 2014, OPM made a sole source award to Imperatis to execute this project.[1042]

As of May 2016, multiple security tools have been purchased—some with only limited due diligence—to secure OPM's legacy IT environment, and a new IT environment has been built (the Shell). After the agency paid a contractor over $45 million for the Tactical and Shell phases, the June 2014 contract was terminated in May 2016 and, as the IG predicted, OPM had two IT environments (legacy and the new Shell) to maintain.[1043] Meanwhile, OPM continues to address concerns first raised by the IG in June 2015 about OPM's contracting approach. Specifically, the IG expressed concern that this investment was made with limited consideration of alternatives and without a full understanding of the scope of existing IT assets and potential costs to execute the entire project.[1044]

The taxpayers' return on this investment is now further in question after the creation of the National Background Investigations Bureau (NBIB), "which will absorb [OPM's] existing Federal Investigative Services (FIS)," and now that the Department of Defense "will assume the responsibility for the design, development, security and operation of the background investigations IT systems for the NBIB."[1045] These developments present a funding challenge for this project because OPM initially planned to rely on funds from OPM's revolving fund,

---

[1040] June 2014 OPM Incident Report at HOGR0818-001233.

[1041] *OPM Data Breach: Hearing Before the H. Comm. On Oversight & Gov't Reform*, 114th Cong. (June 16, 2015) (testimony of Donna Seymour, Chief Information Officer, Office of Personnel Mgmt.).

[1042] Imperatis Letter Contract (June 16, 2014), Attach. 1 at 000002 (Imperatis Production: Sept. 1, 2015).

[1043] OIG Flash Audit Alert (June 17, 2015) at 5 (stating "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."); Email from Imperatis to H. Comm. on Oversight & Gov't Reform Majority Staff (June 7, 2016) (confirming total paid to Imperatis from June 16, 2014 to May 6, 2016 is $45.1 million) (on file with the Committee).

[1044] OIG Flash Audit Alert (June 17, 2015).

[1045] White House, Press Release, *The Way Forward for Federal Background Investigations* (Jan. 22, 2016), https://www.whitehouse.gov/blog/2016/01/22/way-forward-federal-background-investigations.

which is largely derived from background investigation fees OPM collected from other agencies.[1046]

The documents and testimony show OPM's IT Infrastructure project would have benefited from more robust communications with the IG, particularly in responding to cybersecurity incidents. Former OPM CIO Donna Seymour testified she was not aware of a requirement "to notify the IG of every project that we take on."[1047] Given the significant funding for the IT Infrastructure project, which initially had an overall estimated cost of $93 million, the agency-wide nature of this project, and the fact that this project was launched as a consequence of the 2014 data breach, OPM should have involved the OIG so that the expertise of his office could help the agency deter problems before they arose. Because agency did not communicate with the IG on the front end, OPM found itself spending significant time and effort responding to IG concerns after the fact. In this case, the IG found out about the project a year after it was launched.[1048] Shortly thereafter, the IG issued a Flash Audit Alert that contained serious concerns.[1049] The IG and OPM continue to have discussions about these concerns.

The documents and testimony show there should be pre-established contract vehicles for cyber incident response and related services. Instead of issuing a sole source contract to facilitate the procurement of security tools to secure a compromised IT network, in the midst of an emergency situation and without the benefit of competition, there should have been a government-wide contract vehicle already established to fulfill this need. Just as emergency preparedness officials learned the value of establishing contract vehicles to support emergency response to natural disasters prior to such disasters after Hurricane Katrina, so too should similar resources be established for responding to cybersecurity emergencies.[1050]

The state of OPM's IT legacy environment leading up to the 2014 and 2015 breaches illustrates the pressing need for federal agencies to modernize legacy IT in order to mitigate the cybersecurity threat inherent in unsupported, end of life IT systems and applications. The GAO recently observed that in cases where vendors no longer support hardware or software this can create security vulnerabilities and additional costs.[1051] In testimony before the Committee, then-OPM CIO Seymour admitted the vulnerability of OPM's legacy. She stated:

[1046] *OPM Data Breach: Part III: Hearing Before the H. Comm. on Oversight &Gov't Reform* (Feb. 24, 2016) (prepared statement of Norbert E. Vint, Office of Inspector Gen., U.S. Office of Pers. Mgmt.) (hearing cancelled).
[1047] *OPM Data Breach: Part II Hearing Before the H. Comm. on Oversight &Gov't Reform*, 114th Cong. (June 24, 2015) (testimony of Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt.).
[1048] U.S. Office of Personnel Management, Office of Inspector Gen., *Background Information: OPM Infrastructure Overhaul and Migration Project* (June 17, 2015) (on file with the Committee).
[1049] OIG Flash Audit Alert (June 17, 2015).
[1050] In October 2015, OMB released a Cybersecurity Strategy and Implementation Plan (CSIP) that reported an effort to establish a contract vehicle in order to develop a capability to deploy incident response services that could be used by agencies on an expedited basis. Memorandum from Shaun Donovan, Dir., and Tony Scott, Fed. Chief Info. Officer, Office of Mgmt. & Budget, Exec. Office of the President, to Agency Heads, M-16-04, *Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government* (Oct. 30, 2015) available at: https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf.
[1051] Gov't Accountability Office, GAO-16-468, *Information Technology: Federal Agencies Need to Address Aging Legacy Systems* 27(May 2016).

> OPM has procured the tools, both for encryption of its databases, and we are in the process of applying those tools within our environment. But there are some of our legacy systems that may not be capable of accepting those types of encryption in the environment that they exist in today.[1052]

Further, in making the case for updating aspects of OPM's legacy IT environment in the context of this contract, Imperatis said certain servers could no longer be patched and hardware had to be replaced in order to mitigate the risk of catastrophic failure since the current hardware was "woefully out of service."[1053] The need to modernize is clear, however, the modernization of such systems should not be done through a sole source contract in an emergency situation and without a full assessment of alternatives and understanding of the scope and cost of such an effort.

The IG Issues a Flash Audit Alert and Interim Reports on the IT Infrastructure Project

On June 17, 2015, the IG issued a Flash Audit Alert to then-Director Katherine Archuleta on the sole source IT contract to secure and update OPM's legacy IT infrastructure.[1054] The IG raised serious concerns about this project and "identified substantial issues requiring immediate action" and urged the CIO to "immediately begin taking steps to address these concerns."[1055] McFarland wrote:

> [O]ur primary concern is that the OCIO has not followed the U.S. Office of Management and Budget (OMB) requirements and project management best practices. . . the OCIO has initiated this project without a complete understanding of the scope of OPM's existing technical infrastructure or the scale and costs of the effort required to migrate it to the new environment.[1056]

McFarland also expressed concerns "with the nontraditional Government procurement vehicle that was used to secure a sole-source contract with a vendor to manage the infrastructure overhaul."[1057]

These two themes (lack of project management and the sole source contracting approach) have been present throughout the IG's oversight of this project with varying levels of cooperation from OPM. Over time and more recently, OPM officials have become more responsive to the IG's concerns, particularly as new OPM leadership was put in place.

[1052] *OPM Data Breach: Hearing Before the H. Comm. on Oversight & Gov't Reform*, 114th Cong. (June 16, 2015) (testimony of Donna Seymour, Chief Information Officer, Office of Personnel Mgmt.).
[1053] Email from [redacted] Imperatis to Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt. (July 31, 2014, 3:18 p.m.), Attach. 9a at 001163 (Imperatis Production: Sept. 1, 2015); Email from [redacted] Dir. Stragetic Growth, Imperatis to [redacted] U.S. Office of Pers. Mgmt. (Mar. 20, 2015, 3:12 p.m.), Attach 9a at 001170 (Imperatis Production: Sept. 1, 2015).
[1054] OIG Flash Audit Alert (June 17, 2015).
[1055] *Id.* at 1.
[1056] *Id.*
[1057] *Id.*

With respect to the project management concerns, the IG observed at the time that OPM had not "identified the full scope and cost of this project" and had not prepared a Major IT Business case document (which is an OMB requirement for major IT investments).[1058] As a result of the inadequate project management, the IG found "a high risk that this Project will fail to meet the objectives of providing a secure operating environment for OPM systems and applications."[1059] The IG recommended that OPM complete the Major IT Business case document as part of the FY 2017 budget process.[1060]

The IG predicted the failure to plan and understand the full scope of the project also would introduce schedule and cost risks.[1061] For example, OPM did not have a complete IT inventory of existing applications and systems for migration and redesign.[1062] In addition, the cost estimate at the time for the Tactical and Shell phases was approximately $93 million and did not include the cost of migrating legacy applications to the new environment.[1063] The source of funding was also unclear. The IG stated: "when we asked about the funding for the Migration phase, we were told, in essence, that OPM would find the money somehow, and that program offices would be required to fund the migration of applications that they own from their existing budgets."[1064]

With respect to the sole source contract award issue, the IG questioned the use of a sole source contract for all four phases of the network infrastructure improvement project.[1065] The IG acknowledged that the sole source approach may have been appropriate for the first Tactical phase of the project given the immediate need to secure the legacy IT environment.[1066] The IG did not agree, however, that it was appropriate to use this sole source contract for all four phases of the project. Chairman Chaffetz raised those concerns in a June 24, 2015 hearing. He stated: ". . . when it is a sole-source contract, it does beg a lot of questions."[1067]

The IG recommended against using a sole-source contract for all four phases of this project because "without submitting this project to an open competition, OPM has no benchmark to evaluate whether the costs charged by the sole-source vendor are reasonable and appropriate."[1068]

On June 22, 2015, former Director Katherine Archuleta responded to the IG's Flash Audit Alert and generally disagreed with IG's concerns.[1069] She argued that a business case was

---

[1058] OIG Flash Audit Alert (June 17, 2015) at 2.
[1059] *Id.*
[1060] *Id.* at 5.
[1061] *Id.* at 2.
[1062] *Id.* at 3.
[1063] *Id.*
[1064] *Id.*
[1065] *Id.* at 5-6.
[1066] *Id.* at 5.
[1067] *Hearing on OPM Data Breach: Part II* (Statement of Chairman Chaffetz).
[1068] OIG Flash Audit Alert (June 17, 2015) at 6.
[1069] Memorandum from Katherine Archuleta, Dir., U.S. Office of Pers. Mgmt., to Patrick McFarland, Inspector Gen. U.S. Office of Pers. Mgmt., *Response to Flash Audit Alert – U.S. Office of Personnel Management's Infrastructure*

not necessary and would take too long. With respect to the concern that OPM lacked a full understanding of the size, scope, and cost, OPM said: "OPM and the OCIO have always been very clear that the undertaking includes factors and costs that will be understood more clearly as the Project proceeds"—essentially, "we will figure it out as we go."[1070]

OPM also disputed the IG's characterization of the contract as a sole-source award covering all four phases of the IT Infrastructure Improvement project and took the opportunity to state "the contract for the Migration and Cleanup phases of the infrastructure improvement project have not yet been awarded."[1071]

The IG's Concerns Continued through the Fall of 2015

On September 3, 2015, the OIG released an Interim Status Report on the Flash Audit Alert.[1072] The OIG's Interim Status Report acknowledged developments related to this effort that in the IG's view emphasized the need for a "disciplined project management approach."[1073] Such developments included former Director Archuleta's resignation, Senate appropriators' rejection of OPM's $37 million funding request for accelerated migration of IT systems in July 2015, and the fact that OPM had identified "serious security vulnerabilities" in several IT systems, including e-QIP (which is the electronic questionnaire systems for background investigations).[1074]

In the Interim Status Report, the IG reiterated the recommendations in the original Flash Audit Alert and pointed out that OPM has "not yet determined the full scope and overall costs of the Project" and without completing a Major IT Business Case proposal for the Project, the IG concluded "there is a high risk of project failure."[1075] Further, the IG said the sole source award for all four phases and the original justification for making such an award "violate[d] federal acquisition regulations" because "*any* involvement that is not required to correct the urgent and compelling circumstances" would not be justified under the urgent and compelling exception authorizing certain sole source contracts.[1076]

IG Reports Progress in Responding to Concerns, but Challenges Remain as of May 2016

Almost one year after the OPM IG issued a Flash Audit Alert on OPM's IT Infrastructure Improvement project, Acting IG Norbert Vint issued the Second Interim Report on this project in

---

Improvement Project (Report No. 4A-CI-00-15-055) (June 22, 2015)[hereinafter Archuleta Response to IG Flash Audit Alert].

[1070] Archuleta Response to OIG Flash Audit Alert at 3.

[1071] *Id.* at 2.

[1072] Office of the Inspector Gen., U.S. Office of Personnel Mgmt., Report No. 4A-CI-00-15-055, *Interim Status Report on OPM's Responses to the Flash Audit Alert – U.S. Office of Personnel Management's Infrastructure Improvement Project* (Sept. 3, 2015) [hereinafter OIG Interim Status Report (Sept. 3, 2015)].

[1073] *Id.* at 2.

[1074] *Id.* at 1-2.

[1075] *Id.* at 2, 5.

[1076] *Id.* at 7 (emphasis in original) (citing 48 C.F.R. 6.302); 41 U.S.C. 3304(a)(2).

May 2016.[1077] The Acting IG reported some progress with OPM's submission of a major IT Business Case during the FY 2017 budget process, but the Acting IG also said there were lingering overall concerns about the project related to the insufficient capital planning process and unsubstantiated lifecycle cost estimates.[1078] The Acting IG made two recommendations: (1) OPM should conduct an Analysis of Alternatives (AoA) to determine whether the Shell (which is now known as Infrastructure as a Service or IaaS) is the best approach to modernizing the IT environment given changes in the internal and external environments; and (2) OPM should continue to leverage the application profile scoring framework developed by OPM in order to develop reliable cost estimates for modernization and migration activities.[1079]

In May 2016, the Acting IG reported that OPM had submitted a Business Case for this project (as part of the FY 2017 budget process) in response to the IG's prior recommendation. However, after reviewing the document the Acting IG said the document was insufficient because OPM did not perform capital planning activities, such as a performing an AoA to the Shell/Iaas and had not developed a solid cost estimate for modernization and migration.[1080] The Acting IG said OPM still had not determined the full scope of the project, but there had been some improvement in developing an inventory of legacy systems and estimating costs to modernize these systems.[1081]

In addition, the Acting IG identified a new complication to funding the IT Infrastructure Improvement project. Specifically, the decision to create the NBIB and designate the Department of Defense as responsible for the IT systems to support the background investigation process altered the potential funding options. OPM had planned to rely on its revolving fund, which is primarily funded through revenues from the background investigation process, to support the IT Infrastructure Improvement project.[1082] With the creation of the NBIB, the background investigation processing function will no longer be part of the Shell/Iaas. Consequently, this funding source is no longer available.[1083]

The Acting IG concluded that while it was not too late for OPM to complete the capitol planning activities (which should have been done prior to project initiation), the IG remains concerned that "there is a very high risk that the project will fail to meet its stated objectives of delivering a more secure environment at a lower cost."[1084]

On April 22, 2016, OPM's Acting CIO Lisa Schlosser offered OPM's response to the Second Interim Report and said OPM's OCIO "appreciates the detailed analysis and feedback provided in the report and generally concurs with the recommendations."[1085] The OCIO

[1077] Office of Inspector Gen., U.S. Office of Pers. Mgmt., Report No. 4A-CI-00-16-037, *Second Interim Status Report on the U.S. Office of Personnel Mgmt's Infrastructure Improvement Project – Major IT Business Case* (May 18, 2016) [hereinafter OIG Second Interim Status Report on Infrastructure Improvement Project (May 18, 2016)].
[1078] *Id.*
[1079] *Id.* at 5, 8.
[1080] *Id.* at 4.
[1081] *Id.* at 8.
[1082] *Id.* at 5.
[1083] *Id.*
[1084] *Id.* at 5.
[1085] U.S. Office of Personnel Mgmt. Acting Chief Info. Officer Lisa Schlosser *Response* (Apr. 22, 2016) to Office of Inspector Gen., U.S. Office of Pers. Mgmt., Report No. 4A-CI-00-16-037, *Second Interim Status Report on the U.S.*

Response then proceeded to provide details on ongoing efforts and planned next steps to address the IG recommendations. For example, the Acting CIO said, OPM has "engaged in on-going efforts to inventory IT systems and identify plans to mitigate, migrate, or modernize these systems."[1086] Further, OPM agreed that this project would benefit from a more rigorous lifecycle cost estimating process and pointed to a plan to use an application profile framework (developed by OPM's Senior Cybersecurity and IT Advisor) to inform lifecycle cost estimates for IT modernization.[1087]

In sum, OPM has come a long way from the state of affairs in June 2015 when the IG released the Flash Audit Alert on the IT Infrastructure Improvement project. Today, OPM is currently working cooperatively with the IG to mitigate concerns raised by the IG. The agency appears to be making progress on completing basic capitol planning activities that should have been completed prior to the launch of this project and these efforts should be acknowledged. However, the IG continues to have concerns about this project and unfortunately some of the risks identified early on by the IG seem to have played out during the course of the Imperatis contract.

The Story of OPM's IT Infrastructure Improvement Project and the Sole Source Contract

Over the past two years, OPM has made progress toward securing OPM's legacy IT environment and building a new IT environment, but there were significant concerns raised by IG about the IT Infrastructure contract that were validated and expanded upon based on review of the documents obtained by the Committee (which included more than 1,700 pages of documents from Imperatis). The agency did procure updated security tools to secure the legacy IT environment (although not all such interactions were handled through this contract, including Cylance) and the new IT environment (Shell/Iaas) that Imperatis built appears to be an improvement over the legacy IT environment. However, there were schedule and cost challenges (as the IG warned) and questions remain as to how OPM will realize the benefits of new Shell/IaaS and at the same time maintain the legacy IT environment in a cost effective way.

Further, OPM has no clear assessment of whether the costs paid to date under this contract—over $45 million—were reasonable, given the lack of competition for the contract. Finally, the long-term plan for securing and modernizing OPM's IT environment remains unclear, especially given ongoing efforts to complete an analysis of alternatives and establish reasonable cost estimates for modernization.

The following is a timeline of events related to the IT Infrastructure Improvement project contract and more details that validate some of the concerns initially identified by the IG.

Office of Personnel Mgmt's Infrastructure Improvement Project – Major IT Business Case at 1 [hereinafter Schlosser Response to Second Interim Status Report].

[1086] Schlosser Response to Second Interim Status Report (Apr. 22, 2016) at 1.

[1087] *Id.* at 3.

Timeline: OPM's IT Infrastructure Improvement Project

- May 10, 2014. Then-OPM CIO Donna Seymour contacts former colleagues (who she knew from her time at the U.S. Maritime Administration (around 2006)) at Imperatis, about the IT security situation at OPM and a potential IT project to address the situation.[1088]

- May 27, 2014. In response to the malicious activity identified in March 2014, OPM executes the "Big Bang" remediation plan. OPM's Director of IT Security Operations, Jeff Wagner and DHS/US-CERT team members provided an unclassified briefing to Imperatis employees.[1089]

- June 16, 2014. Letter contract statement of objectives for Imperatis contract describes activities under the contract in **all four phases** of the IT Infrastructure Improvement project.[1090] The base year of the contract plus options included a period from June 2014 through December 2016. Initially, $18 million was allocated under the letter contract.

- June 22, 2014. DHS/US-CERT issues the OPM Incident Report and makes fourteen recommendations to improve OPM's IT security, including a general recommendation to "redesign their network architecture to incorporate security best practices."[1091]

- October 14, 2014. Solicitation for IT Infrastructure Improvement contract issued as part of the process to definitize the June 2014 Letter contract.[1092]

- November 12, 2014. Imperatis submits a proposal in response to October 14, 2014 solicitation.[1093]

- January 30, 2015. Imperatis contract for OPM's IT Infrastructure Improvement project is definitized.[1094]

- February 2015. OPM FY 2016 Congressional Budget Justification requests $21 million "to implement and sustain agency network upgrades initiated in FY 2014 and security

---

[1088] Email from Donna Seymour, Chief Info Officer, U.S. Office of Pers. Mgmt., to Patrick Mulvaney and [redacted] Imperatis (May 10, 2014, 9:46 a.m.), Attach. 12 at 001463 (Imperatis Production: Sept. 1, 2015).

[1089] Letter from Maj. General (ret.) Mastin Robeson, President & Chief Exec. Officer, Imperatis Corp. to the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform (Sept. 1, 2015) at 8.

[1090] Imperatis Letter Contract (June 16, 2014), Attach. 1 at 000002 (Imperatis Production: Sept. 1, 2015). OPM used a DHS contract vehicle, but the former OPM CIO Donna Seymour was designated the contracting officer representative (COR) and thus was responsible for contract performance management. *Id.* at 000011 (designating Ms. Seymour as COR).

[1091] June 2014 OPM Incident Report at HOGR0818-001236.

[1092] Letter from Maj. General (ret.) Mastin Robeson, President & Chief Exec. Officer, Imperatis Corp. to the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform (Sept. 1, 2015) at 9.

[1093] Imperatis Proposal Volume I – Statement of Work and Technical, Attach. 5 at 000178 (Imperatis Production: Sept. 1, 2015).

[1094] Imperatis Definitized Contract (Jan. 30, 2015), Attach. 2 at 000040 (Imperatis Production: Sept. 1, 2015).

software maintenance to ensure a stronger, more reliable, and better protected OPM network architecture."[1095]

- March 27, 2015. Imperatis coordinates initial meeting with CyTech and OPM to evaluate CyTech's CyFIR tool for possible use in the new IT Infrastructure (the Shell).[1096]

- March 2015. OIG becomes aware of the IT Infrastructure Improvement Project when the OCIO meet with OIG to discuss the special assessment the OCIO would be collecting from all OPM program offices to partially fund the project.[1097]

- April 2, 2015. CyTech meets with Imperatis and OPM at CyTech office in Manassas.[1098]

- April 15, 2015. OPM notifies US-CERT regarding potential indicators of compromise.[1099]

- April 21-22, 2015. CyTech product demonstration at OPM facilitated by Imperatis.[1100]

- June 15, 2015. The first six month option to continue Shell (phase 2) work is exercised. This option expired December 15, 2015.[1101]

- June 16, 2015. The Committee holds first hearing on the OPM data breach.[1102]

- June 17, 2015. IG McFarland issues Flash Audit Alert to then-Director Archuleta to alert her to "serious concerns" the IG has regarding the OCIO infrastructure improvement project. The IG finds OCIO launched project "without a complete understanding of the scope of OPM's existing technical infrastructure or the scale and costs of the effort required to migrate it to the new environment." The IG also expresses concern that a sole source contract award had been made.[1103]

[1095] U.S. Office of Pers. Mgmt., *OPM Congressional Budget Justification Performance Budget FY2016*, at 2 (Feb. 2015), available at: https://www.opm.gov/about-us/budget-performance/budgets/congressional-budget-justification-fy2016.pdf.

[1096] Imperatis Weekly Report (Mar. 30, 2015-Apr. 3, 2015), Attach.6 at 000704 (Imperatis Production: Sept. 1, 2015).

[1097] U.S. Office of Personnel Management, Office of Inspector Gen. *Background Information: OPM Infrastructure Overhaul and Migration Project* (June 17, 2015) (on file with the Committee).

[1098] Imperatis Response to H. Comm. on Overisght & Gov't Reform Majority Staff Regarding Clarification on Sept. 1, 2015 Production (Sept. 10, 2015) (on file with the Committee).

[1099] AAR Timeline – Unknown SSL Certificate (April 15, 2015) at HOGR020316-1922-23 (OPM Production: Apr. 29, 2016).

[1100] Imperatis Response to H. Comm. on Overisght & Gov't Reform Majority Staff Regarding Clarification on Sept. 1, 2015 Production (Sept. 10, 2015) (on file with the Committee).

[1101] Memorandum from the Hon. Beth Cobert, Act. Dir, U.S. Office of Personnel Mgmt. to Patrick McFarland, Inspector Gen., U.S. Office of Pers. Mgmt., *Response to Interim Status Report on OPM's Responses to the Flash Audit Alert – U.S. Office of Personnel Management's Infrastructure Improvement Plan (Report No. 4A-CI-00-15-055)* (Sept. 9, 2015) at 3.

[1102] *OPM Data Breach: Hearing Before the H. Comm. On Oversight and Gov't Reform*, 114th Cong. (June 16, 2015).

[1103] OIG Flash Audit Alert (June 17, 2015).

- June 22, 2015. Then-Director Archuleta responds to IG's Flash Audit Alert regarding the IT Infrastructure Improvement Project. OPM generally disagrees with the recommendations in the Flash Audit Alert, saying there was no time to do a business case and activities associated with the Shell are extensions of existing IT investments.[1104]

- June 24, 2015. The Committee holds a second hearing on the OPM data breach. Then-CIO Donna Seymour testifies "we only contracted for the first two pieces" of the four-phase IT Infrastructure Improvement project. She also says the estimated cost of the initial project phases was $93 million.[1105]

- July 22, 2015. OPM IG McFarland issues a memorandum to Acting Director Cobert on serious concerns regarding the CIO, including CIO's statement to Congress that she was "not aware of a requirement . . . to notify the IG of every project we take on" (in response to a question about the IT Infrastructure Improvement project) and incorrect/misleading information provided by OPM on the sole source contract.[1106]

- August 18, 2015. Committee sends letter to Imperatis requesting information about the IT Infrastructure Improvement project.[1107]

- September 1, 2015. Imperatis provides documents to the Committee in response to August 18 request.[1108]

- September 3, 2015. OIG issues Interim Status Report on the Flash Audit Alert on OPM's IT Infrastructure Improvement project.[1109]

- September 9, 2015. Acting Director Cobert responds to the IG's September 3 Interim Status Report on IT Infrastructure Improvement project.[1110]

- September 17, 2015. Imperatis completes buying cybersecurity tools to secure the legacy IT environment (Tactical Phase 1).[1111]

[1104] Archuleta Response to OIG Flash Audit Alert.
[1105] *Hearing on OPM Data Breach Part II* (testimony of Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt.).
[1106] OIG Serious Concerns Regarding OCIO (July 22, 2015).
[1107] Letter from the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform to Major General (ret.) Mastin Robeson, President & Chief Exec. Officer, Imperatis (Aug. 18, 2015).
[1108] Letter from Maj. General (ret.) Mastin Robeson, President & Chief Exec. Officer, Imperatis to the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform (Sept. 1, 2015).
[1109] OIG Interim Status Report (Sept. 3, 2015).
[1110] Memorandum from the Hon. Beth Cobert, Act. Dir, U.S. Office of Personnel Mgmt. to Patrick McFarland, Inspector Gen., U.S. Office of Pers. Mgmt., *Response to Interim Status Report on OPM's Responses to the Flash Audit Alert – U.S. Office of Personnel Management's Infrastructure Improvement Plan (Report No. 4A-CI-00-15-055)* (Sept. 9, 2015).
[1111] Imperatis Response to H. Comm. on Overisght & Gov't Reform Majority Staff Questions on Status of the Project (Feb. 12, 2016) (on file with the Committee).

- September 28, 2015. Imperatis completes initial operational capability of the Shell (Phase 2). Imperatis had planned to complete Full Operational Capability early summer 2016. Performance tuning and staff training on new technologies for the Shell were planned to continue through the end of the contract period of performance (December 2016).[1112]

- October 15, 2015. Imperatis provides briefing to Committee staff on their interactions with CyTech and status of the IT Infrastructure Improvement project.

- December 10, 2015. Chairman Chaffetz calls for Seymour to resign for the sixth time citing, in addition to previous concerns, IT Infrastructure Improvement project concerns.[1113]

- January 22, 2016. The White House announces the creation of the NBIB "which will absorb [OPM's] existing Federal Investigative Services (FIS)" and stated the Defense Department "will assume the responsibility for the design, development, security and operation of the background investigations IT systems for the NBIB."[1114]

- February 24, 2016. OPM Acting IG Norbert Vint prepared testimony for a Committee hearing, entitled "OPM Data Breach: Part III" (canceled) and highlighted continuing concerns about the IT Infrastructure Improvement Project and the sole source contract.[1115]

- April 22, 2016. OPM Acting CIO Lisa Schlosser issues a memorandum to the OIG responding to a draft of the Second Interim Status Report on the IT Infrastructure Improvement project and outlining next steps to implement the IG's recommendations.[1116]

- May 6, 2016. Imperatis reports payments from OPM totaling $45.1 million for the period June 16, 2014 through May 6, 2016.[1117]

- May 9, 2016. OPM terminates Imperatis' contract for nonperformance. Imperatis is precluded from public comment due to Non-Disclosure Agreement with OPM.[1118]

[1112] Imperatis Response to H. Comm. on Overisght & Gov't Reform Majority Staff Questions on Status of the Project (Feb. 12, 2016) (on file with the Committee).

[1113] Letter from the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform to Beth Cobert, Acting Dir., U.S. Office of Pers. Mgmt. (Dec. 10, 2015).

[1114] White House, Press Release, *The Way Forward for Federal Background Investigations* (Jan. 22, 2016), available at: https://www.whitehouse.gov/blog/2016/01/22/way-forward-federal-background-investigations.

[1115] *OPM Data Breaches: Part III: Hearing Before H. Comm. on Oversight & Gov't Reform*, 114th Cong. (Feb. 24, 2016) (prepared statement of Norbert E. Vint, Office of Inspector Gen., U.S. Office of Pers. Mgmt. OPM) (cancelled).

[1116] Schlosser Response to Second Interim Status Report (Apr. 22, 2016).

[1117] Email from Impertis to H. Comm. on Oversight & Gov't Reform Majority Staff (June 7, 2016) (on file with the Committee).

[1118] Jack Moore, *Contractor Working on OPM's Cyber Upgrades Suddenly Quits, Citing "Financial Distress,"* NEXTGOV (May 13, 2016), available at: http://www.nextgov.com/cybersecurity/2016/05/contractor-working-opms-cyber-upgrades-suddenly-quits-citing-financial-distress/128301/. Based on information provided to the Committee

- May 18, 2016. The Acting IG issues the Second Interim Status Report on the IT Infrastructure Improvement project noting continuing concern regarding the lack of critical capital project planning practices required by OMB for this project, but also noting some positive actions by OPM.[1119]

- June 2016. Original end date for the first option period for the Imperatis contract.

- December 2016. Original end date for the second option period for the Imperatis contract.

OPM Initiates Contact with Imperatis and Awards Sole Source Contract

On May 10, 2014, then-OPM CIO Donna Seymour initiated contact with two Imperatis employees with whom she had previously worked on a prior IT project at the U.S. Maritime Administration.[1120] She explained that she was looking for assistance to help "straighten out a very messy network with poor security."[1121] Initially, Seymour offered to hire one of these individuals as an OPM employee, but he declined, citing a commitment to his supervisor at Imperatis, and offered instead to provide assistance as an expert consultant.[1122] Seymour said she would investigate potential options for such assistance, adding: "I want/need you on the team."[1123]

OPM and Imperatis continued discussions about the scope of the project and potential costs through late May.[1124] Then on May 27, 2014, Imperatis received an unclassified briefing from Jeff Wagner, OPM's Director of IT Security Operations and members of the US-CERT team regarding the network security incident OPM learned about in March 2014.[1125] In a letter to the Committee, Imperatis told the Committee that this briefing "conveyed an urgent and compelling need for immediate action on both the operational network . . . and for the development of a new, separate and distinct information systems architecture."[1126]

---

the contractor may be experiencing financial difficulty due to an accounting issue for a separate and unrelated contract with another agency.

[1119] OIG Second Interim Status Report on Infrastrcuture Improvement Project (May 18, 2016).

[1120] Email from Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt., to Patrick Mulvaney, Senior IT Manager and [redacted] Dir. of Strategic Growth, Imperatis (May 10, 2014, 9:46 a.m.), Attach. 12 at 001463 (Imperatis Production: Sept. 1, 2015).

[1121] *Id.*

[1122] Email from Patrick Mulvaney, Senior IT Manager, Imperatis, to Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt. (May 12, 2014, 10:01 a.m.), Attach 12 at 001479 (Imperatis Production: Sept. 1, 2015).

[1123] Email from Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt., to Patrick Mulvaney, Senior IT Manager, Imperatis (May 12, 2014, 10:10 a.m.), Attach. 12 at 001479 (Imperatis Production: Sept. 1, 2015).

[1124] For example, on May 17, 2014 Imperatis provided labor rates information to Ms. Seymour. *See* Email from [redacted] Dir. of Strategic Growth, Imperatis to Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt. (May 17, 2014, 11:14 a.m.), Attach. 12 at 001482 (Imperatis Production: Sept. 1, 2015).

[1125] Letter from Maj. General (ret.) Mastin Robeson, President & Chief Exec. Officer, Imperatis to the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform (Sept. 1, 2015) at 8.

[1126] *Id.* Imperatis also noted that a decision was made to use a DHS contracting vehicle given their cybersecurity role for the federal government. *Id.*

On June 16, 2014 (just over one month after initially contacting Imperatis), a letter contract award was made to Imperatis.[1127] In the days leading up to this award, Wagner followed up on a phone call with Imperatis. He emailed: "I am looking forward to having you guys come in. My team and I have been working this issue with no funding and limited assistance for four years. It will be awesome to have better opinions and solutions."[1128] Wagner testified to the Committee that "Imperatis was contracted to build out a new environment, and in building out the new environment they were given the initiative to find new technologies and innovation."[1129]

Imperatis and OPM Buy Security Tools to Secure the Legacy IT Environment

Documents obtained by the Committee from Imperatis show a list of ten tools that OPM purchased through the Imperatis contract to secure OPM's legacy network.[1130] Purchases were made beginning in June 2014 up through October 2014.[1131] There were challenges in deploying tools, including delays and technical challenges.[1132] The documents show the time elapsed between the purchase of these tools and completing deployment ranged from almost three to fifteen months.[1133]

The reasons for the extended period of time between purchase and full deployment varied and are not entirely clear from the record. Wagner testified that when OPM rolled out certain tools, such as PIV cards, these deployments "caused certain applications and certain functionalities to break, and it was something that we had to work through."[1134]

Further, in the case of completing the roll out of a tool called ForeScout, the documents show some delay can be attributed to a requirement for "notifications" to applicable unions. ForeScout, which is a tool to manage network access control for devices, was purchased in July

---

[1127] Imperatis Letter Contract (June 16, 2014), Attach. 1 at 000002 (Imperatis Production: Sept. 1, 2015); Email from [redacted] Contracting Officer, Dep't of Homeland Sec., to [redacted] Imperatis (June 16, 2014, 3:41 p.m.) at 001556-1598 (Imperatis production: Sept. 1, 2015).

[1128] Email from Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt., to Patrick Mulvaney, Senior IT Manager, Imperatis (June 13, 2014, 1:59 p.m.), Attach. 12 at 001539 (Imperatis Production: Sept. 1, 2015).

[1129] Wagner Tr. at 97.

[1130] OPM Tactical Toolset Purchase, Kick-off and Completion Timeframes (Oct. 21, 2015) (Imperatis Supplemental Document Production: Oct. 21, 2015) (on file with the Committee).

[1131] *Id.*

[1132] Imperatis told the Committee their role in buying security tools during the Tactical phase of the contract "was limited to acting as a procurement agent to purchase OPM-selected security tools and associated vendor professional services." Letter from Maj. General (ret.) Mastin Robeson, President & Chief Exec. Officer, Imperatis to the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform (Sept. 1, 2015) at 4. The record indicates that Imperatis while acting as an agent also provided justification for tools and typically did perform some due diligence on these purchases. Email from [redacted] Imperatis, to Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt. (July 29, 2014, 3:10 p.m.), Attach. 9a at 1160-1161 (Imperatis Production: Sept. 1, 2015) (explaining the benefits of Palo Alto Networks Next Generation Firewalls).

[1133] OPM Tactical Toolset Purchase, Kick-off and Completion Timeframes (Oct. 21, 2015) (Imperatis Supplemental Document Production: October 21, 2015) (on file with the Committee).

[1134] Wagner Tr. at 72.

2014, but it was not fully deployed until September 2015.[1135] Imperatis stated in a Weekly Report for August 2015 that "approval has not yet been received for Agency-wide memo" and "project sponsor is in notification stage with the Union."[1136] The mitigation strategy for this situation was to "prepare updated project timeline, plan & memo to pilot ForeScout to Non-Union Agency users."[1137]

The documents show there were also situations where Imperatis was not able to perform due diligence because of the expedited nature of a purchase. For example, in July 2014 Imperatis described a risk/challenge area: "OPM's desire to purchase tactical gear without Imperatis being able to perform true due diligence on tool and fit into current 'as is' network."[1138] Part of the proposed mitigation strategy for this challenge was to collect more information from Wagner and request his assistance in setting priorities.[1139] This limitation on due diligence and lack of priorities was identified as a Risk/ Challenge beginning in July 2014 through November 2014 until Imperatis stated "implementations are proceeding and most roadblocks have been cleared."[1140]

Imperatis' Role in Responding to OPM Data Breach Incidents

Imperatis stated to the Committee that they did not perform incident response activities related to the June and July 2015 data breach announcements.[1141] Imperatis said OPM and other OPM contractors were responsible for operations, security, and maintenance of the legacy IT environment. The record does show other contractors with a more significant role in incident response and security of the legacy IT environment.[1142] Imperatis did facilitate meetings with vendors, who played a role in incident response and also did provide "24 man-hours of assistance for security incident response and clean up," according to a Report for the Week of April 27, 2015.[1143] While Imperatis did not perform significant incident response activities, they did have some visibility into the incident response and the IT security challenges related to the data breach incidents announced in 2015.

Imperatis was aware of the March 2014 security incident as demonstrated by documents provided to the Committee. For example, documents show Imperatis was invited to assist OPM

[1135] OPM Tactical Toolset Purchase, Kick-off and Completion Timeframes (Oct. 21, 2015) (Imperatis Supplemental Document Production: October 21, 2015) (on file with the Committee).
[1136] Imperatis Weekly Report (Aug. 3, 2015-Aug. 7, 2015), Attach. 6 at 000942 (Imperatis Production: Sept. 1, 2015).
[1137] *Id.*
[1138] Imperatis Weekly Report (July 8, 2014-July 14, 2014), Attach. 6 at 000342 (Imperatis Production: Sept. 1, 2015).
[1139] *Id.*
[1140] Imperatis Weekly Report (Nov. 10, 2014-Nov. 14, 2014), Attach. 6 at 000478 (Imperatis Production: Sept. 1, 2015);Id, Attach. 6 at 000492 (Imperatis Production: Sept. 1, 2015).
[1141] Letter from Maj. General (ret.) Mastin Robeson, President & Chief Exec. Officer, Imperatis to the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform (Sept. 1, 2015) at 12.
[1142] Saulsbury, an employee of SRA explained his role at OPM saying he had worked at OPM since 2012 as an SRA contractor and worked in network security. He said, SRA provides "supplemental staffing" under a contract to provide a variety of IT management services. Saulsbury Tr. at 8-10.
[1143] Imperatis Weekly Report (Apr. 27, 2015-May 1, 2015), Attach. 6 at 000758 (Imperatis Production: Sept. 1, 2015).

after the primary incident response period for the March 2014 incident.[1144] The Imperatis proposal also stated: "Unfortunately, OPM experienced a recent security incident that occurred because the network was neither set up to easily recognize potential intrusions nor quickly react with the necessary incident response to stop attacks from becoming major data breaches."[1145] Imperatis said by the time of the June and July 2015 OPM breach announcements, the procurement of security tools for OPM's legacy network under the Tactical phase of this project was "nearly 100 % complete."[1146] Imperatis said they did not generally provide incident response services during this period.[1147] However, Imperatis did report that at OPM's request during this period Imperatis "arrange[d] the procurement of Palo Alto firewalls and associated professional services to support the bolstering of network defense around the e-QIP applications" and completed this procurement by July 1, 2015.[1148]

Sole Source, Schedule, and Cost IG Concerns Related to OPM's IT Infrastructure Improvement Contract Validated

Documents and testimony obtained by the Committee show:

OPM Officials Made Statements to Congress that were Inconsistent with the Record.

When the IG raised concerns about OPM making a sole source award for all four phases of the IT Infrastructure Improvement project, OPM officials insisted that a contract award had not been made for the latter two phases of the project (Migration and Clean-Up). Then-CIO Donna Seymour testified before the Committee that "we only contracted for the first two pieces" of this multi-phased project.[1149] Former Director Katherine Archuleta made similar statements before the Committee and elsewhere.[1150]

[1144] Letter from Maj. General (ret.) Mastin Robeson, President & Chief Exec. Officer, Imperatis to the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform (Sept. 1, 2015) at 7-8.

[1145] Imperatis Proposal Volume II – Staffing and Mangement, Attach. 5a at 000233 (Imperatis Production: Sept. 1, 2015).

[1146] Letter from Maj. General (ret.) Mastin Robeson, President & Chief Exec. Officer, Imperatis to the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform (Sept. 1, 2015) at 12.

[1147] *Id.*

[1148] *Id.* Note 1: The e-QIP (Electronic Questionnaire for Investigations Processing System) is used to collect information related to Federal background investigations. On June 29, 2015, OPM shut down the E-QIP system, which was offline until August 4, 2015. Assistant IG Michael Esser said of the shut down, "OPM's official statement on this issue claims that the agency is acting proactively by shutting down the E-QIP system. However, the current security review ordered for this system is a direct reaction to the recent security breaches. In fact, the e-QIP system contains vulnerabilities that OPM knew about, but had failed to correct for years." *Is the OPM Data Breach the Tip of the Iceberg?: Hearing Before* the *Hearing Before Subcomm. on Research & Tech. and Subcomm. on Oversight of the H. Comm. on Science, Space & Tech.*, 114th Cong. (July 8, 2015) (statement of Michael Esser, Assistant Inspector Gen., U.S. Office of Pers. Mgmt.). Note 2: An OPM constructed diagram of how the attacker navigated OPM's system identified [redacted] as one of the affected servers. *See* OPM data breach diagram dated Sept. 1, 2015 at HOGR07264-000947-ur (unredacted version of OPM production: Dec. 22, 2015). An OPM contractor noted in a transcribed interview that he believed [redacted] "related to accessing E-QIP" (Saulsbury Tr. At 76).

[1149] *Hearing OPM Data Breach Part II* (testimony of Donna Seymour, Chief Information Officer, Office of Personnel Management).

[1150] *Hearing OPM Data Breach Part II* (stating "I would like to remind him [the IG] that the contracts for Migration and Cleanup have not yet been awarded."); *Hearing on OPM Information Technology Spending and Data Security*

Later, OPM admitted the contractor did have a role in the latter two phases of the IT Infrastructure Improvement project. On September 3, 2015, Acting Director Cobert supplemented the former Director's response to the IG regarding the sole-source contract and Imperatis' role in the later phases (Migration and Clean up) of the project.[1151] Acting Director Cobert explained that "although the contract contemplates that Imperatis will have work to do in all four phases, not all aspects of the work required by OPM in phases three and four is included in the contract with Imperatis."[1152]

The documents show that while not all work for the project is covered, OPM did in fact make a sole source contract award to Imperatis for work in *all four phases* of OPM's IT Infrastructure Improvement project. Thus, from the beginning, this sole-source award was to cover aspects of work from all four phases of this project. Indeed, the IG pointed out in the June 17 Flash Audit Alert that the original documentation justifying the sole source award covered all four phases of the work (Tactical, Shell, Migration and Clean Up).[1153] The IG also pointed out that in a May 26, 2015 meeting, the former CIO argued in favor of an approach where the same contractor oversaw all four phases of the project.[1154]

The Committee obtained the contract file, which calls into the question the truthfulness of certain statements by OPM officials to Congress. The contract documents outlined in detail the contractor's role in each of the four phases of this project. The Statement of Objectives (SOO) for the June 2014 letter contract states "the work is focused in four primary phases" and then listed tasks that the Contractor was expected to perform under each phase.[1155] For the Migration phase, the SOO stated, "Contractor shall work with OPM to plan for, oversee, and assist in the migration of existing OPM network and business applications and services into the new IT infrastructure."[1156] For the Clean Up phase, the SOO stated, "Contractor shall work with OPM to cleanse all data and applications from unused hardware and shall prepare it to be excessed."[1157] The Statement of Work (SOW) for the contract stated, "[t]he Contractor shall complete work within this SOW in four different phases: Tactical, Shell, Migration, and Clean Up."[1158] The SOW also is similar to the SOO in that the SOW outlines specific contractor tasks in the later two phases of the project.[1159]

(stating "I would like to remind the Inspector General that contracts for the Migration and Cleanup have not yet been awarded.").

[1151] Memorandum from the Hon. Beth Cobert, Acting Dir., U.S. Office of Pers. Mgmt. to Patrick McFarland, Inspector Gen., U.S. Office of Pers. Mgmt., *Supplement to Response to Flash Audit Alert – U.S. Office of Personnel Mgmt's Infrastructure Improvement Project (Report No. 4A-CI-00-15-055)* (Sept. 3, 2015) [hereinafter Cobert Response (Sept. 3, 2015) to OIG Interim Status Report].

[1152] Cobert Response (Sept. 3, 2015) to OIG Interim Status Report at 1.

[1153] OIG Flash Audit Alert (June 17, 2015) at 5-6.

[1154] *Id.*

[1155] Imperatis Letter Contract Statement of Objectives (June 16, 2014), Attach. 1 at 000007 (Imperatis Production: Sept. 1, 2015).

[1156] *Id.*

[1157] *Id.*

[1158] Imperatis Definitized Contract Statement of Work (Jan. 15, 2015), Attach. 1 at 000077 (Imperatis Production: Sept. 1, 2015).

[1159] *Id. at 81.*

The Committee obtained documents that show the contractor had every expectation that they would be providing services through all four phases of the project. In their November 2014 proposal, the contractor said, "[o]ur response to the SOW directly responds to each of the four phases of the program and describes the ways in which our team has begun fulfilling these requirements to date" and added that their proposal provided "a detailed response and solution to each of the four phases of the Infrastructure Improvement program."[1160] In addition, the contractor outlined in their proposal a five step process with an illustrative diagram for the Migration phase.[1161]

Finally, as the contractor began to perform under the contract, the documents show the contractor was performing tasks related to the later phases of the project. In February 2015, the contractor first identified "stand up of Migration PMO office" as a high risk area and proposed a strategy to mitigate potential risks to include "working closely with ACIOs to ensure IT program managers & application teams are engaged with project plans and a migration schedule is in place."[1162] In early April 2015, the contractor's Weekly Report included a "Migration Process" diagram and discussion of "Migration: Phase 2 options" with pros and cons.[1163] In May 2015, the contractor provided updates on the Migration PMO office saying "Initial engagement happened. There were 2 questions from the application groups."[1164] These activities clearly show the contractor understood the work covered under this contract included tasks related to the Migration phase.[1165]

The IG's Concerns about Schedule Risks Were Validated.

In the June 2015 Flash Audit Alert, the IG raised a concern that OPM had significantly underestimated the time to complete the Migration (Phase 3) of this project and did not consider the complexity and lengthy process to complete this phase.[1166] According to the IG's Alert, OPM estimated the Migration of all of OPM's legacy applications/systems would take eighteen to twenty-four months. Imperatis immediately recognized the schedule challenges and identified schedule risk as a concern in the proposal they submitted. Imperatis's proposal stated: "the duration of the current period of performance is insufficient to accomplish a complete migration into Shell."[1167]

[1160] Imperatis Proposal Volume II – Staffing and Mangement ,Attach. 5a at 000233 (Imperatis Production: Sept. 1, 2015).
[1161] *Id.* at 000222.
[1162] Imperatis Weekly Report (Feb. 16, 2015-Feb. 20, 2015), Attach. 6 at 000649 (Imperatis Production: Sept. 1, 2015).
[1163] Imperatis Weekly Report (Apr. 6, 2015-Apr. 10, 2015), Attach 6 at 000718-20 (Imperatis Production: Sept. 1, 2015).
[1164] Imperatis Weekly Report (May 4, 2015-May 8, 2015), Attach. 6 at 000774 (Imperatis Production: Sept. 1, 2015).
[1165] Imperatis stated in a letter to the Committee that while they were engaged in some role for all four phases of the project, their most significant work related to the Shell – or Phase 2. Letter from Maj. General (ret.) Mastin Robeson, President & Chief Exec. Officer, Imperatis to the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform (Sept. 1, 2015) at 3.
[1166] OIG Flash Audit Alert (June 17, 2015) at 3.
[1167] Imperatis Proposal Volume I – Statement of Work and Technical, Attach. 5 at 000219 (Imperatis Production: Sept. 1, 2015).

Imperatis also cited, in particular, challenges with applications requiring modernization, including the Federal Investigative Services and Retirement Services.[1168] These applications alone are complex and will take significant time and effort to migrate to modernized solutions.

Two years after the June 2014 award, the tactical phase has been completed, a new IT environment appears to have been delivered (but perhaps not fully tested/trained on), and OPM is still working to inventory and fully scope the alternatives of mitigating or migrating OPM's legacy IT to the new Shell/IaaS. Saulsbury testified to the Committee that he did not work on the Shell, but reported that "Imperatis has some of the infrastructure up and running" and added "Imperatis is starting to train SRA staff on how to operate some of the tools within the shell environment."[1169]

The IG's Concerns about Cost Risks Were Validated.

In the June 2015 Flash Audit Alert, the IG also said there was significant cost "uncertainty" with this project due to the unknown scope of the work required, including a full inventory of OPM's IT assets.[1170] According to Weekly Progress report documents obtained by the Committee, the contractor identified funding for the Shell phase as an area of high risk beginning in February 2015 through at least August 2015.[1171] From March 2015 through April 2015, the contractor updated this high risk area by saying, "still awaiting Mod for additional funding."[1172] In early May 2015 the contractor reported "Mod received. Now discussing additional material funding needed for the rest of FY and FY 2016 through Dec. 15th."[1173] Then in July through August 2015, the contractor update was "need additional funding quickly to ensure no delay in procurement."[1174] The documents show funding for the Shell was a significant ongoing concern.

The uncertainty with respect to total cost of this project has persisted, although OPM now appears to be taking constructive action aimed at improving long term cost estimates. In the June 2015 Flash Audit Alert, the IG reported that OPM had estimated the Tactical (Phase 1) and Shell (Phase 2) portions of the project could cost approximately $93 million, which included $67 million to be collected from major OPM programs as a "special assessment" with little information as to the scope of the project.[1175]

[1168] *Id.*
[1169] Saulsbury Tr. at 11.
[1170] OIG Flash Audit Alert (June 17, 2015) at 3.
[1171] Imperatis Weekly Report (Feb. 23, 2015- Feb. 27, 2015), Attach. 6 at 000658 (Imperatis Production: Sept., 1, 2015); Imperatis Weekly Report (Aug. 10, 2015- Aug. 14, 2015) , Attach. 6 at 000958 (Imperatis Production: Sept. 1, 2015).
[1172] Imperatis Weekly Report (Mar. 23, 2015- Mar. 27, 2015), Attach. 6 at 000700 (Imperatis Production: Sept. 1, 2015); Imperatis Weekly Report (Apr. 20, 2015- Apr. 24, 2015), Attach. 6 at 000746 (Imperatis Production: Sept. 1, 2015).
[1173] Imperatis Weekly Report (Apr. 27, 2015 to May 1, 2015), Attach. 6 at 000760 (Imperatis Production: Sept. 1, 2015).
[1174] Imperatis Weekly Report (July 13, 2015- July 17, 2015), Attach. 6 at 000910 (Imperatis Production: Sept. 1, 2015); Imperatis Weekly Report (Aug. 10, 2015-Aug. 14, 2015), Attach. 6 at 000958 (Imperatis Production: Sept. 1, 2015).
[1175] OIG Flash Audit Alert (June 17, 2015) at 3.

As of late October 2015, OPM reported to the Committee that overall it had spent about $60 million in FY2014 and 2015 for this project.[1176] The contractor has reported being paid a total of $45.1 million for the period of June 16, 2014 through May 6, 2016. [1177]

In May 2016, the IG reported that OPM's FY 2017 Business Case for this project outlined costs already incurred with some "reasonable short-term estimates to finish developing the IaaS portion [Shell]."[1178] However, the IG expressed concerns about the cost estimates for the long term efforts to modernize and migrate to a new IT environment—and called these estimates "unsubstantiated because of the incomplete inventory and technical analysis." At the same time, the IG did acknowledge as positive, OPM efforts to develop cost estimates for modernizing and /or migrating all OPM information systems by leveraging a new application profiling scoring framework.[1179]

In January 2016, the Administration announced the creation of the NBIB and the designation of the Department of Defense (DOD) as responsible for the IT security of background investigation data. This announcement has further complicated efforts to identify a definitive plan to fund IT modernization at OPM given that OPM's background investigation program is being moved to the NBIB and DOD will be responsible for IT security and funding for these functions likely will not be available for modernizing other OPM IT assets.[1180]

The Status and Future Plans for OPM's New IT Environment (Shell/Iaas) are Unclear.

In the June 2015 Flash Audit Alert, the OIG predicted OPM could find itself in a situation where it could be incurring costs to maintain two IT environments (legacy and the Shell). In June 2015, the IG said without a disciplined planning process or a guaranteed funding source in place to complete this likely complex and expensive process, "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."[1181] The OIG added such a scenario would be inconsistent with the goal of "creating a more secure IT environment at a lower cost."[1182] This appears to now be the case with the creation of the Shell and continued uncertainty about plans and costs for mitigation, modernization and/or migration of OPM's legacy IT environment.

The goal of achieving a more secure environment at lower costs appears to be at risk. In May 2016, the OIG reported that OPM had allocated a "limited amount of funding" to

---

[1176] Email from U.S. Office of Pers. Mgmt. to H. Comm. on Oversight & Gov't Affairs (Oct. 28, 2015) (on file with the Committee).
[1177] Imperatis Response to H. Comm. on Overisght & Gov't Reform Majority Staff (June 7, 2016) (on file with the Committee).
[1178] OIG Second Interim Status Report on Infrastructure Improvement Project at 7.
[1179] Office of Inspector Gen., U.S. Office of Pers. Mgmt., Report No. 4A-CI-00-16-037, *Second Interim Status Report on the U.S. Office of Personnel Mgmt's Infrastructure Improvement Project – Major IT Business Case* at 8 (May 18, 2016).
[1180] *OPM Data Breaches: Part III: Hearing Before H. Comm. on Oversight & Gov't Reform*, 114th Cong. (Feb. 24, 2016) (prepared statement of Norbert E. Vint, Office of Inspector Gen., U.S. Office of Pers. Mgmt.) (cancelled).
[1181] OIG Flash Audit Alert (June 17, 2015) at 5.
[1182] *Id.*

modernization and migration efforts.[1183] According to the IG, OPM's Business Case for the IT Infrastructure Improvement project allocated only twenty to twenty-five percent of this project's cost for modernization/migration with the remainder allocated to securing and maintaining the legacy and IaaS/Shell environment. The OIG questioned this approach because it does not acknowledge "maintenance cost for the dual environments will not likely remain fixed."[1184] The OIG speculated that as the costs to maintain the legacy environment increase, this could result in limited funding for modernization and migration. Meanwhile, OPM is now currently spending approximately $25 million annually to maintain the IaaS/Shell.[1185]

According to the OIG, OPM is considering a plan to save money by physically moving legacy systems from old data center environments to the new environment.[1186] Such a plan would include keeping the legacy systems in a separate logical environment from Shell/IaaS. It is reasonable to consider such a plan for the purposes of saving money, but as the IG pointed out serious consideration should be given to the security risks of "maintaining security controls in two logical environments indefinitely."[1187]

In sum, OPM's IT Infrastructure Improvement project, which was motivated by the laudable goals of securing the legacy IT environment and creating a more secure lower cost modernized IT environment, fell victim to a flawed contracting and planning approach. Two years after this effort began and after much time and effort to acknowledge and mitigate OIG concerns, OPM is only now making progress toward a disciplined planning and assessment of the alternatives and establishing a reasonable cost estimating process.

[1183] OIG Second Interim Status Report on Infrastructure Improvement Project at 7.
[1184] *Id.*
[1185] *Id.* at 8.
[1186] *Id.* at 7-8.
[1187] *Id.* at 8.

Summary of Investigation

The agency's posture with respect to the Committee's investigation has been consistently uncooperative until the later stages of the investigation, especially as it compares to the level of cooperation from other agencies and contractors who had relevant documents and information.

Committee hearings on the data breaches

On June 16, 2015, the Committee held its first hearing on the OPM data breach, which was entitled "OPM: Data Breach."[1188] The hearing occurred twelve days after OPM publicly announced the breach of personnel records for "approximately four million" current and former federal employees.[1189] The hearing included testimony from witnesses from OPM, the OPM OIG, the OMB, DHS, and DOI. This hearing provided the Committee an opportunity to learn what occurred, based on the information available at that time, but responses from some witnesses increased concerns about the data breach. Following the hearing, Members were invited to a classified briefing on the data breaches.

Twenty days after OPM announced the breach affecting personnel records, the Committee convened a hearing on June 24, 2015, entitled "OPM Data Breach: Part II."[1190] The Committee heard testimony from OPM, the OPM OIG, U.S. Investigations Services, LLC (a former OPM background investigation contractor), and KeyPoint Government Solutions (a current OPM background investigation contractor). During the June 24 hearing, the Committee received an update on the investigation and learned background investigation data also had been compromised, but OPM declined to provide specific information on the number of individuals impacted, citing an ongoing investigation. The Committee also learned more about the OPM data breach discovered in March 2014. Specifically, the Committee heard testimony that "manuals about the servers and environment" had been taken from OPM's network during the incident.[1191] Then-CIO Donna Seymour admitted the "manuals about the servers and the environment" would provide "enough information that [the adversary] could learn about the platform, the infrastructure of [OPM's] system."[1192]

On the same day as the second hearing, then-OPM Director Archuleta sent a letter to Chairman Chaffetz clarifying the number of former and current federal employees' whose personnel records were compromised by saying roughly 4.2 million individuals were impacted and stating an unspecified number of former and current federal employees' background investigation data had been compromised.[1193] It was not until July 9, 2015 that OPM publicly announced the background investigation data of 21.5 million current, former, and prospective

---

[1188] *OPM: Data Breach: Hearing Before the H. Comm. on Oversight & Gov't Reform*, 114th Cong. (June 16, 2015).
[1189] U.S. Office of Pers. Mgmt., Press Release, *OPM to Notify Employees of Cybersecurity Incident* (June 4, 2015), https://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident/
[1190] *Hearing on OPM Data Breach: Part II.*
[1191] *Id.*
[1192] *Id.*
[1193] Letter from Katherine Archuleta, Dir., U.S. Office of Personnel Mgmt., to the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform (June 24, 2015).

federal employees, contractors, and related non-applicants had been compromised.[1194]

Then on July 15, 2015 (just over a month after the breach was first announced), the Committee's Subcommittee on Information Technology and Subcommittee on the Interior held a joint hearing, entitled "Cybersecurity at the U.S. Department of Interior."[1195] Since DOI held OPM personnel records that were stolen in a shared service data center facility, this hearing allowed the Committee to better understand the impact of the breach on DOI, how its systems interacted with those of OPM, and more detail about how the breach occurred. The agency's CIO and Inspector General testified.

In order to learn more about the incidents described at these hearings, the Committee continued its investigation and made multiple requests for information and documents from relevant stakeholders.

Committee request for information regarding identity theft services

On July 21, 2015, Chairman Chaffetz and Ranking Member Cummings sent the first letter to OPM requesting information about: (1) the contract for the identity theft protection services for 4.2 million current and former federal employees' whose personnel record data had been compromised and; (2) OPM's plans to provide identity theft services to the 21.5 million individuals whose background investigation data had been compromised.[1196]

On August 21, 2015, OPM provided an initial response related to the identity theft contract for the 4.2 million personnel records victims to the Committee.[1197] OPM declined to provide detailed information regarding plans for an identity theft services contract for the 21.5 million until a contract had been awarded.

On September 1, 2015, OPM and the Department of Defense (DOD) announced a new identity theft protection and credit monitoring contract award to provide identity theft services to

---

[1194] U.S. Office of Personnel Mgmt., Press Release, *OPM Announced Steps to Protect Federal Workers and others from Cyber Threats* (July 9, 2015) available at: https://www.opm.gov/news/releases/2015/07/opm-announces-steps-to-protect-federal-workers-and-others-from-cyber-threats/

[1195] *Cybersecurity: The Department of the Interior: Hearing Before the Subcomm. on Info.Tech. and Subcomm. on Interior of the H. Comm. on Oversight & Gov't Reform*, 114th Cong. (July 15, 2015).

[1196] Letter from the Hon. Jason Chaffetz, Chairman, and the Hon. Elijah E. Cummings, Ranking Member, H. Comm. on Oversight & Gov't Reform, to the Hon. Beth Cobert, Acting Dir, U.S. Office of Pers. Mgmt. (July 21, 2015).

[1197] The Committee reviewed the documents OPM provided and confirmed the contract award to Winvale/CSID was not a sole-source award as was originally suggested. However, as the IG later reported there were some contracting irregularities, but it was unclear whether these irregularities would have changed the awardee. On December 2, 2015, the IG completed a Special Review (in response to the Committee's request during the June 24, 2015 hearing) on the $20 million contract to provide credit monitoring and identity protection services to the initial 4.2 million victims of the OPM data breach. The IG's Special Review determined "that in order to meet the OCIO's June 8, 2015, requirements due date, the contracting officer failed to comply with FAR requirements and OPM policies and procedures in awarding the Winvale contract" and then the IG identified five areas of noncompliance. Office of the Inspector Gen., U.S. Office of Pers. Mgmt., 4K-RS-00-16-024, *Special Review of OPM's Award of a Credit Monitoring and Identity Theft Services Contract to Winvale Group LLC and its Subcontractor, CSIdentity*, (Dec. 2, 2014).

the 21.5 million individuals impacted by the background investigation data breach.[1198] After further inquiries to OPM regarding the contract information, OPM deferred to DOD for the details of this contract. The Committee obtained relevant records from DOD on October 20, 2015.[1199]

The DOD award was made under a government-wide contract vehicle established by the General Services Administration (GSA). This contract vehicle provides agencies with access to contractors capable of providing identity monitoring, data breach response, and protection services. This contract vehicle is available to agencies for up to five years and has an estimated value of $500 million. In contrast to the first contract arrangement for the 4.2 million individuals, the September 1, 2015 contract award established a government-wide vehicle for these services so that agencies are not trying to establish a contracting vehicle to provide identity theft services in the middle of incident response. DOD handled the notification process directly for the 21.5 million victims and the initial notification process was completed in December 2015.[1200]

Productions related to the OPM data breaches and CyTech

On July 24, 2015, Chairman Chaffetz and Ranking Member Cummings sent a second letter to OPM requesting information and documents in response to questions about specific details of the data breaches announced in June and July 2015.[1201] The letter covered a range of issues, including information about OPM's relationship with, and the work conducted by, CyTech Services; information on OPM security tools and user credentials for OPM information systems; and additional information related to the data breach.

The request related to CyTech was prompted by a referral from the House Permanent Select Committee on Intelligence (HPSCI) and press reports. On June 15, 2015, the *Wall Street Journal* published a story on the OPM data breaches, alleging that CyTech had discovered the breach during the demonstration of their security tool.[1202] Then on June 23, 2015, just before the Committee's second hearing on the OPM data breaches where the Committee heard testimony about CyTech, the Committee received a memorandum from Rep. Devin Nunes, Chairman of

---

[1198] U.S. Office of Pers. Mgmt., Press Release, *OPM, DOD Announce Identity Theft Protection and Credit Monitoring Contract* (Sept. 1, 2015), available at: https://www.opm.gov/news/releases/2015/09/opm-dod-announce-identity-theft-protection-and-credit-monitoring-contract/.

[1199] Letter from the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform, to the Hon. Ray Mabus, Sec., Office of the Sec. of the Navy (Sept. 22, 2015); Letter from R. L. Thomas, Dir., Navy Staff, Dep't of the Navy, Dep't of Defense to the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform (Oct. 20, 2015).

[1200] In the Consolidated Appropriations Act for Fiscal Year 2016, language was including requiring OPM to provide individuals impacted by the OPM data breach with 10 years of identity protection services (versus three years under the Sept. 1, 2015 award) and five million in liability insurance. Jason Miller, *Pay raise, transit benefits parity gives feds optimism for 2016*, FEDERAL NEWS RADIO, Dec. 17, 2016.

[1201] Letter from the Hon. Jason Chaffetz, Chairman, and the Hon. Elijah E. Cummings, Ranking Member, H. Comm. on Oversight & Gov't Reform, to the Hon. Beth Cobert, Acting Director, U.S. Office of Pers. Mgmt. (July 24, 2015).

[1202] Damian Paletta, *Cybersecurity Firm Says It Found Spyware on Government Network in April,* WALL ST. J., June 15, 2015, available at: http://www.wsj.com/articles/firm-tells-of-spyware-discovery-in-government-computers-1434369994.

HPSCI, and Rep. Adam Schiff, HPSCI's Ranking Member, regarding the information from CyTech.[1203]



THE WALL STREET JOURNAL.

Home World U.S. Politics Economy Business Tech Markets Opinion Arts Life Real Estate

U.S. POLITICS NATIONAL SECURITY

Cybersecurity Firm Says It Found Spyware on Government Network in April

CyTech Services's claim raises questions over how personnel-data theft was discovered

As a result of these events, the Committee sought documents and information to better understand the facts and any role CyTech played at OPM during the 2015 incident response period. Pursuant to this effort, the Committee requested information from OPM about CyTech as part of a broader July 24, 2015 letter to OPM. On August 14, 2015 Chairman Chaffetz also sent an information request to Ben Cotton, Chief Executive Officer of CyTech.[1204] The letter requested all documents and communications between OPM and CyTech, details about the product demonstration that CyTech conducted at OPM in April 2015, and any additional activities conducted by CyTech related to incident response.[1205] CyTech responded to this request on August 19, 2015 by providing documents to Committee staff during a visit to CyTech headquarters in Manassas, Virginia. The Committee also conducted a transcribed interview with Cotton on September 30, 2015.[1206]

While CyTech promptly responded to the Committee's request for information, OPM dragged its feet. OPM's initial response to the Committee's July 24, 2015 letter did not include information in response to questions about CyTech.[1207] On September 25, 2015, OPM made a second production in response to the July 24, 2015 request, producing a nine-page narrative in response to questions posed about CyTech and only one relevant document—more than 175 pages of visitor logs from OPM's Washington, D.C. headquarters for the month of April 2015 that were almost entirely redacted.[1208]

[1203] Letter from the Hon. Devin Nunes, Chairman, and the Hon. Adam Schiff, Ranking Member, H. Permanent Select Committee on Intelligence, to the Hon. Jason Chaffetz, Chairman, and the Hon. Elijah E. Cummings, Ranking Member, H. Comm. on Oversight & Gov't Reform (June 23, 2015).

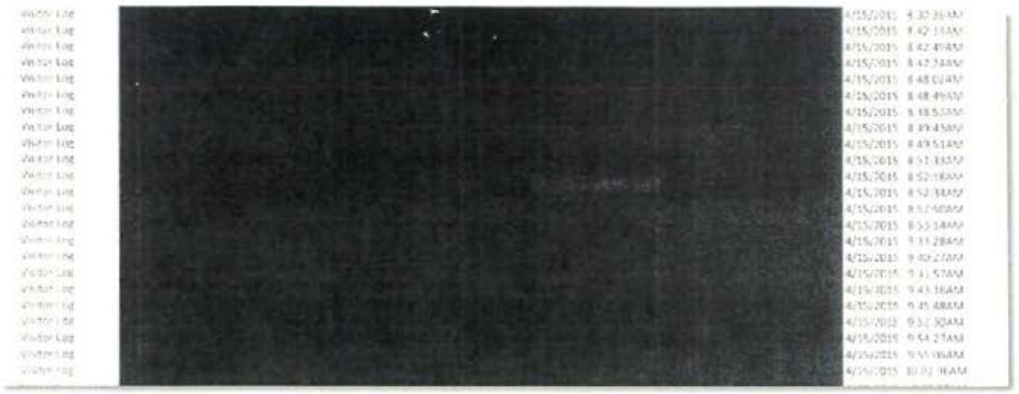
[1204] Letter from the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform, to Ben Cotton, President & Chief Exec. Officer, CyTech (Aug. 14, 2015) (Ranking Member Cummings did not sign this request).

[1205] Letter from the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform, to Ben Cotton, President & Chief Exec. Officer, CyTech (Aug. 14, 2015).

[1206] Cotton Transcribed Interview.

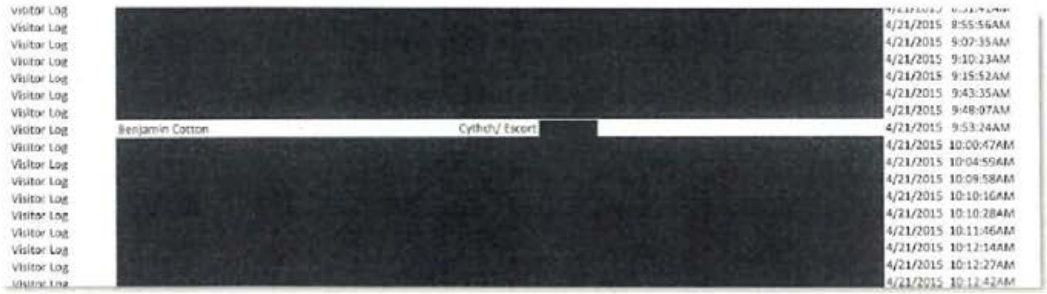
[1207] August 28, 2015 (OPM document production).

[1208] Letter from Jason Levine, Dir. of Cong., Legislative & Intergovernmental Affairs, U.S. Office of Pers.Mgmt., to the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform (Sept. 25, 2015) (OPM Production: Sept. 25, 2015); Office of Personnel Management Visitor Log April 1- July 10, 2015 at HOGR724000325-501 (OPM Production, Sept. 25, 2015).



Heavily redacted visitor logs provided by OPM on September 25, 2015

OPM made a third production to the Committee on October 7, 2015 that included a slightly less redacted version of the visitor logs and a corresponding analysis of entries for staff from CyTech, Imperatis, DHS and the FBI.[1209]



On October 28, 2015, OPM made a substantial production of (redacted) documents, made documents available *in camera*, and responded to a September 9, 2015 letter regarding a "deleted drive" on CyTech's CyFIR appliance.[1210] On August 19, 2015, CyTech told Committee staff it had requested the CyFIR appliance be returned multiple times, but it was not returned until August 20, 2015[1211]—one day after Committee investigators visited CyTech offices.

The CyFIR appliance was returned to CyTech sanitized, that is, with all information deleted.[1212] The agency did not provide a copy of the drive's contents to the Committee, despite the fact that there was an ongoing congressional investigation and preservation order in place. The status of the deleted contents of the drive, and whether OPM preserved a copy, was

---

[1209] Office of Personnel Management Visitor Log April 1-July 10, 2015 at HOGR0724-000615-791 (OPM Document Production: Oct. 8, 2015). Additional responsive documents were also made available to the Committee *in-camera* in the OPM liaison office at this time.

[1210] Letter from the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform and the Hon. Michael Turner, to the Hon. Beth Cobert, Acting Dir., U.S. Office of Pers. Mgmt. (Sept. 9, 2015).

[1211] Cotton Tr. at 72.

[1212] Email from Brendan Saulsbury, Senior Cyber Security Engineer, SRA to Jonathan Tonda, SRA, U.S. Office of Pers. Mgmt. and Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt. (Aug. 17, 2015, 1:54 p.m.) at HOGR0909-000107 (OPM Production: Oct. 28, 2015).

discussed at length at a January 7, 2016 Committee hearing.[1213] It was not until April 2016, that OPM made a sample of the images collected by CyFIR available for an *in camera* review. OPM had obtained this information for the *in camera* review from US-CERT.



Chairman Chaffetz questions an OPM witness about redactions

Despite Committee requests for information and an August 21, 2015 preservation order, OPM did not preserve all relevant evidence. The preservation order covered all records related to the breach/intrusion, the infrastructure improvement project, cybersecurity, and decisions on implementing the recommendations made by the OIG.[1214]

As a result of documents produced by CyTech, and interviews with CyTech employees, the Committee obtained evidence related to the efforts of other firms involved in the April 2015 incident response activities at OPM, including Cylance, SRA, and Imperatis. Each of these companies was present throughout the incident response period and ultimately provided information useful in understanding the bigger picture of what unfolded before, during, and after the OPM data breaches.

The Committee investigated the role of Cylance

Cylance was first identified during a review of documents provided by CyTech. In an April 24, 2015 email, an employee of Cylance, Chris Coulter, emailed CyTech's CEO to ask: "Would you be able [to] pull this file, want to verify something . . . ."[1215] In a September 28,

---

[1213] *Document Production Status Update: Hearing Before the H. Comm. on Oversight & Gov't Reform*, 114th Cong. (Jan. 7, 2016) at 1:07.

[1214] Letter from the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform, to the Hon. Beth Cobert, Dir., U.S. Office of Pers. Mgmt. (Aug. 21, 2015).

[1215] E-mail from Chris Coulter, Managing Dir., Cylance, to Benjamin Cotton, Chief Exec. Officer, CyTech (Apr. 24, 2015, 1:54 p.m.) at 1.27 (CyTech Production: Aug. 19, 2015).

2015 briefing to Committee staff, OPM's Director of IT Security Operations, Jeff Wagner, told staff that Cylance executed the quarantine order on OPM's systems in April 2015.

On December 3, 2015, the Committee sent a letter to Cylance inquiring about the activities it conducted at OPM in April 2015 and requested related documents.[1216] Cylance provided thousands of pages of documents on a rolling basis and in a timely manner, and also made available to the Committee a virtual data room with additional pieces of information and evidence.

The Committee subsequently conducted transcribed interviews of two Cylance personnel.[1217] The Committee conducted a transcribed interview with Cylance CEO Stuart McClure on February 4, 2016. On February 12, 2016, the Committee conducted a transcribed interview with Cylance Managing Director of Incident Response and Forensics Chris Coulter. Coulter was heavily involved in providing assistance to OPM with the deployment of Cylance tools.

The Committee investigated the role of SRA

SRA, International, another OPM contractor, provided information that helped inform a more complete picture of the OPM data breach incidents identified in March 2014 and April 2015.[1218] The Committee was able to identify two key SRA employees who provided OPM IT security operations contract support in 2014 and 2015.[1219] The SRA employees provided IT security operations center support under an SRA contract for IT management services and reported to OPM's Director of IT Security Operations, Jeff Wagner.

The Committee contacted one of these SRA employees, Brendan Saulsbury, who responded to questions about his role in the OPM data breach incident response in an informal interview in January 2016. Later, on February 16, 2016, Saulsbury participated in a transcribed interview.[1220] Saulsbury started with SRA in early 2012 and by March 2012 began providing IT security operations support to OPM under an SRA contract. Saulsbury administered various IT security tools and played a key role in the 2014 and 2015 OPM data breach incident response and forensic investigation. The other (now former) SRA employee identified through the Committee's investigation, Jonathan Tonda, began working for OPM as a federal employee in the Fall of 2015. As of May 2016, Saulsbury left SRA and is employed with another organization.

[1216] Letter from the Hon. Jason Chaffetz, Chairman, and the Hon. Elijah E. Cummings, Ranking Member, H. Comm. on Oversight & Gov't Reform, to Stuart McClure, Chief Exec. Officer, Cylance (Dec. 3, 2015).
[1217] McClure Tr.; Coulter Tr.
[1218] SRA International has combined with the North American Public Sector business of CSC to form SRA in the fall of 2015. *See* CSC, Press Release, *CSC to Combine Government Services Unit with SRA Upon Separation from CSC; Combination Will Create Leading Pure-Play Government I.T. Business in the U.S.* (Aug. 31, 2015).
[1219] E-mail from Brendan Saulsbury, Contractor for OPM IT Security Operations, to Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt. (June 11, 2015, 11:44 p.m.) (CyTech Production Aug. 19, 2015).
[1220] Saulsbury Tr.

The Committee Investigated OPM's IT Infrastructure Improvement Project and the Contract Awardee Imperatis

On June 17, 2015, OPM's IG issued a Flash Audit Alert to then-Director Katherine Archuleta regarding OPM's contract award to Imperatis for the IT Infrastructure Improvement project.[1221] This contract was awarded in June 2014 as part of OPM's response to the data breach discovered in March 2014. The Committee requested follow up information from the IG and raised further questions about this contract, based on the Flash Audit Alert during the June 24, 2015 hearing.[1222] The Flash Audit Alert also led the Committee to review the Imperatis contract and its role in activities at OPM in April/May 2015 related to the data breach incident response. As part of Imperatis activities for the Tactical (Phase 1) portion of the IT Infrastructure Improvement project, Imperatis coordinated meetings with CyTech and OPM and ultimately CyTech's demonstration of its CyFIR tool at OPM on April 21, 2015. The CEO of CyTech identified key Imperatis personnel onsite for demonstration, which assisted the investigation.

Chairman Chaffetz sent an August 18, 2015 letter to Imperatis requesting documents and communications related to CyTech and the IG's Flash Audit Alert.[1223] On September 1, 2015, Imperatis responded to the Chairman's request and produced over 1,700 pages on the IT Infrastructure Improvement project contract, including information on pre-contract communications between OPM and Imperatis employees, the security tools tested and deployed, and contract performance.[1224] In addition, Imperatis provided a briefing to Committee staff on October 15, 2015, explaining its role in scheduling and participating in the CyTech demonstration. Finally, Imperatis responded to supplemental requests by majority staff on contract developments and clarifications on its document production.

Document productions by Department of Homeland Security

On August 19, 2015, Chairman Chaffetz sent a letter to US-CERT requesting information and documents related to its role in assisting OPM with incident response and the forensics investigation of the data breaches identified in March 2014 and Spring 2015.[1225] US-CERT was reluctant to provide documents directly and quickly because US-CERT expressed a preference that OPM provide all US-CERT documents directly to the Committee due to its view that the documents were similar to a client's information. Regardless of this view, it is US-CERT's responsibility to fully respond in a timely manner to congressional information requests. The Committee ultimately received a production of over 350 pages from US-CERT on December 11, 2015 – nearly four months after the initial request.[1226] The delay in receiving this information

[1221] OIG Flash Audit Alert (June 17, 2015).
[1222] *OPM Data Breach: Part II* (June 24, 2015).
[1223] Letter from the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform to Major General (ret.) Mastin Robeson, President & Chief Exec. Officer, Imperatis (Aug. 18, 2015).
[1224] Letter from Maj. General (ret.) Mastin Robeson, President & Chief Exec. Officer, Imperatis to the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform (Sept. 1, 2015).
[1225] Letter from the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform, to Ann Barron-DiCamillo, Dir., U.S. Comp. Emergency Readiness Team, U.S. Dep't of Homeland Sec. (Aug. 19, 2015).
[1226] Letter from M. Tia Johnson, Ass't Sec't for Legislative Affairs, U.S. Dep't. of Homeland Sec. to the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform (Dec. 11, 2015).

could have been avoided had OPM and US-CERT been more timely and responsive to Committee requests.

Unnecessary delays, restrictions, redactions and a congressional subpoena

From July 2015 until early spring of 2016, OPM provided sluggish and incomplete responses to requests, offering only *in-camera* review of certain documents, and documents that were often riddled with redactions. Further, OPM finally produced key documents with limited redactions to the Committee just a few days before the Committee conducted a transcribed interview with OPM's Director of IT Security Operations, Jeff Wagner on February 18, 2016.[1227]

Unnecessary delays

Of the multiple information requests sent to OPM prior to the February 3, 2016, subpoena, not a single one was answered completely within the requested timeframe. This lack of cooperation slowed the Committee's investigation and resulted in the Committee having to make multiple requests to other stakeholders.

For example, on August 18, 2015, Chairman Chaffetz sent another letter to OPM regarding the "stolen manuals" issue and requested a response by September 1, 2015.[1228] The letter referenced June 24, 2015 hearing testimony from then-CIO Donna Seymour responding to the Chairman's questions about the exfiltration of security documents and manuals related to OPM's network.[1229] The letter requested documents and communications about the incident and the information that was stolen.[1230]

When OPM responded on September 18, 2015, the response contained significant redactions.[1231] In fact, it was not until January 12, 2016 (nearly five months after the initial letter was sent) and after a congressional hearing where Members of the Committee expressed frustration about the redactions, that OPM made the unredacted documents available *in camera*. OPM finally produced these documents to the Committee without redactions on February 16, 2016. The stolen manual production was critical to understanding more about the data breach discovered in March 2014.

Unnecessary redactions

The agency routinely provided the Committee with documents containing unnecessary redactions. In addition to the aforementioned visitor logs that were redacted to the point of

---

[1227] Wagner Tr. at 23.
[1228] Letter from the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform, to the Hon. Beth Cobert, Acting Dir., U.S. Office of Pers. Mgmt. (Aug. 18, 2015).
[1229] *Id.*
[1230] *Id.*
[1231] Letter from Jason Levine, Dir., Cong., Legislative & Intergovernmental Affairs, Office of Pers. Mgmt., to the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform (Sept. 18, 2015).

initially being useless,[1232] the agency redacted the name of OPM press officials in some cases.[1233] There is no valid basis for OPM to redact the name of its press officials, especially given their very public role in communicating with the press and public.

In another example, OPM redacted the name of the contracting officer who was managing the first contract for the identity protection services for breach victims.[1234] The agency redacted the name of the officer despite the fact that his name was publicly available on a now archived Fed BizOps website page.[1235] Further, the Committee requested the *curriculum vitae* of Jeff Wagner, OPM's Director of Security Operations, in its July 24, 2015, letter to OPM.[1236] When OPM responded to the request over a month letter, OPM redacted Wagner's name.[1237]



Director of the Office of Congressional Affairs Jason Levine testifies before the Committee

[1232] OPM redacted virtually every name on the visitor logs it provided the Committee pursuant to the July 24, 2015 letter's second request.
[1233] E-mail from [redacted], to Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt (June 12, 2015, 1:50 p.m.), at HOGR020316-000211 (OPM Production Feb. 16, 2016).
[1234] Winvale Contract (June 2, 2015) at 028 (OPM Production: Aug. 21, 2015).
[1235] Solicitation Number: OPM3215T0019 (May 28, 2015) available at: https://www.fbo.gov/index?s=opportunity&mode=form&id=ebef7df6fb8783dbc59c977962833760&tab=core&tabmode=list&print_preview=1.
[1236] Letter from the Hon. Jason Chaffetz, Chairman, and the Hon. Elijah E. Cummings, Ranking Member, H. Comm. on Oversight & Gov't Reform, to the Hon. Beth Cobert, Acting Dir., U.S. Office of Pers. Mgmt. (July 24, 2015).
[1237] Letter from Jason Levine, Dir., Cong., Legislative & Intergovernmental Affairs, U.S. Office of Pers. Mgmt., to the Hon. Jason Chaffetz, Chairman, and the Hon. Elijah E. Cummings, Ranking Member, H. Comm. on Oversight & Gov't Reform (Aug. 28, 2015), (OPM Production: Aug. 28, 2015).

Subpoena issued to OPM

In a January 7, 2016 hearing before the Committee, Jason Levine, Director of the Office of Congressional, Legislative and Intergovernmental Affairs at OPM testified that "OPM has worked tirelessly . . . to respond to numerous congressional inquiries regarding the incidents" and that "OPM has made every effort to work in good faith to respond to multiple congressional oversight requests, including document productions."[1238]

Seven months after the Committee's first request to OPM for information, the Committee issued a subpoena on February 3, 2016, to compel the agency to produce unredacted documents on a permanent basis.[1239] As outlined above, the Committee invested significant time and effort in attempting to extract documents and relevant information from OPM in the months leading up to the February 3, 2016 subpoena.[1240] While OPM did eventually produce requested documents without redactions directly to the Committee, it was only after multiple rounds of productions and significant time and effort to extract these documents from OPM. The fact is that OPM failed to fully cooperate with this investigation until a subpoena triggered greater cooperation.

In contrast to OPM, other relevant stakeholders contacted by the Committee were cooperative and responsive to the Committee's requests. The Committee received documents from contractors and other relevant entities that it would receive from OPM months later. For example, CyTech provided documents to the Committee on August 19, 2015, that included email conversations between OPM's Director of Security Operations, Jeff Wagner, and CyTech CEO Ben Cotton regarding the *Wall Street Journal* story on CyTech.[1241] The agency produced this same document in February 2016 (after the subpoena had been issued).[1242] In another example, CyTech produced an email in August 2015 that led the Committee to investigate Cylance's role in the incident response activities in April 2015 that OPM only produced in February 2016.[1243]

[1238] *Document Production Status Update: Hearing Before the H. Comm. on Oversight & Gov't Reform*, 114th Cong., (Jan. 7, 2016) (Statement of Jason K. Levine, Dir., Office of Cong.l, Legislative, and Intergovernmental Affairs, U.S. Office of Pers. Mgmt.).

[1239] Subpoena from the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform, to Beth Cobert, Acting Dir., U.S. Office of Personnel Mgmt., (Feb. 3, 2016).

[1240] *Id.*

[1241] Cotton Tr., Ex. 10 (Email from Ben Cotton, Chief Exec. Officer, CyTech, to Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt. (June 12, 2015)).

[1242] Email from Ben Cotton, Chief Exec. Officer, CyTech, to Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt. (June 12, 2015, 1:07 p.m.) at HOGR020316-000205 (OPM Production: Feb. 16, 2016).

[1243] Cotton Tr., Ex. 5 (Email from Chris Coulter, Managing Dir., Cylance, to Ben Cotton, Chief Exec. Officer, CyTech (Apr. 24, 2015)); Email from Chris Coulter, Managing Dir., Cylance, to Ben Cotton, Chief Exec. Officer, CyTech (Apr. 24, 2015, 5:54 p.m.) at HOGR020316-000010 (OPM Production: Feb. 16, 2016).

Conclusion

The devastating consequences of OPM cyberattacks discovered in 2014 and 2015 will be felt by the country for decades to come. The key question now before the country is how will we respond? Federal agencies, including OPM, must remain vigilant in protecting the information of hundreds of millions of Americans and in an environment where a single vulnerability is all a sophisticated actor needs to steal or alter Americans' information, the identities of average Americans, and profoundly damage the interests of U.S. national security.

The longstanding inability of OPM to adequately implement sometimes basic, but necessary security measures, despite years of warnings from its Inspector General, represents a failure of culture and leadership, not technology. However, the Committee remains hopeful that OPM, under the new leadership of Acting Director Beth Cobert, is in the process of remedying decades of mismanagement.

In late June 2016, OPM reported to the Committee that over the past year "OPM has taken significant steps to enhance its cybersecurity posture, protect individuals who had their data stolen in the incidents last summer, and reestablish confidence in its ability to deliver on OPM's core missions."[1244] OPM reports such steps include:

- Completing deployment of two-factor Strong Authentication for all users, which provides a strong barrier to OPM's networks from individuals that should not have access;
- Implementing a continuous monitoring program for all IT systems;
- Creating and hiring a cybersecurity advisor position that reports to the Director;
- Establishing an agency-wide centralized IT security workforce under a newly hired Chief Information Security Officer (CISO);
- Modifying the OPM network to limit remote access to exclusively government-owned computers;
- Deploying new cybersecurity tools, including software that prevents malicious programs and viruses on our networks;
- Implementing a Data Loss Prevention System which automatically stops sensitive information, such as social security numbers from leaving the network unless authorized; and
- Enhancing cybersecurity awareness training with emphasis on Phishing emails and other user based social engineering attacks.[1245]

OPM also reports that it has taken steps to improve its cybersecurity capabilities, many of which are part of the President's Cybersecurity National Action Plan. In particular, OPM reports being one of the first agencies to fully implement DHS' Continuous Diagnostics and Mitigation (CDM) program, and that it is targeted to complete its deployment by the end of summer 2016. OPM reports that CDM will allow OPM to communicate with DHS more rapidly and effectively

[1244] Email from Jason Levine, Dir., Office of Cong., Legislative, & Intergovernmental Affairs, U.S. Office of Pers. Mgmt., to H. Comm. on Oversight & Gov't Reform Staff (June 21, 2016, 6:54 p.m.) (on file with the Committee).
[1245] *Id.*

during cybersecurity incidents. In addition, OPM has also completed the implementation of the latest release of Einstein – Release 3a, which is a DHS IT defensive system that collects, detects, and prevents many cyber threats and potential cyber-attacks before they can reach OPM networks and its users.[1246]

But questions remain as to the state and utility of OPM's new information technology infrastructure. How will the newly established National Background Investigations Bureau (NBIB) impact the new IT infrastructure that OPM has built, and that was designed for the Federal Investigative Service which will now belong to the DOD-administered NBIB? Such questions linger as OPM continues to spend tens of millions to maintain and operate both their existing legacy IT environment and the new IT infrastructure. Only time will tell if OPM is able to sufficiently respond to the call for the agency to address its information security shortcomings and IT challenges, especially given the reality that federal CIOs have an average tenure of only two years.[1247]

As Representative Will Hurd, Chairman of the Information Technology subcommittee, stated during the first hearing, the data breach at OPM this "is just another example of the undeniable fact that America is under constant attack. It is not bombs dropping or missiles launching; it is the constant stream of cyber weapons aimed at our data."[1248] OPM and all federal agencies must overcome the unique challenges that each faces with regard to their information environments. Every American must have the confidence that the data they continue to entrust with the federal government will be protected. Agency leadership and their CIOs must be the ones to restore the public trust following the events that transpired at OPM.

[1246] Id.

[1247] Gov't Accountability Office, GAO-11-634, *Federal Chief Information Officers: Opportunities Exist to Improve Role in Information Technology Management* (Oct. 2011).

[1248] *OPM Data Breach: Hearing Before H. Comm. on Oversight and Gov't Reform*, 114th Cong. (June 16, 2015) (Statement of Rep. Will Hurd).

Appendix: Cyber security Spending at OPM (Fiscal Years 2012-2015)

Table 1. Federal cybersecurity spending by agency (in millions) for FY2015[1249]

Agency	Prevent Malicious Cyber Activity	Detect, Analyze, and Mitigate Intrusions	Shaping the Cybersecurity Environment	Total
Department of Agriculture	$39	$39	$5	$83
Department of Commerce	$43	$79	$71	$194
Department of Education	$8	$18	$0	$27
Department of Energy	$130	$105	$68	$303
Department of Justice	$291	$131	$35	$456
Department of Labor	$6	$12	$4	$22
Department of State	$102	$73	$25	$200
Department of Transportation	$41	$49	$5	$95
Department of Veterans Affairs	$96	$89	$25	$210
Department of the Interior	$13	$20	$28	$61
Department of the Treasury	$159	$96	$16	$271
Department of Defense	$3,200	$1,100	$4,800	$9,100
Department of Health & Human Services	$71	$132	$17	$220
Department of Homeland Security	$316	$771	$225	$1,313
Department of Housing & Urban Development	$7	$8	$1	$15
Environmental Protection Agency	$2	$12	$3	$17
General Services Administration	$16	$24	$6	$46
International Assistance Programs	$8	$8	$5	$22
National Science Foundation	$3	$6	$206	$215
National Aeronautics & Space Administration	$30	$54	$23	$107
Nuclear Regulatory Commission	$8	$13	$3	$25
Office of Personnel Management	$2	$5	$0	$7
Small Business Administration	$2	$8	$0	$10
Social Security Administration	$51	$38	$2	$91
Total Cybersecurity Spending	**$4,646**	**$2,887**	**$5,577**	**$13,110**

NOTE: Due to rounding, categories may not sum to the total

[1249] Office of Mgmt. & Budget, Exec. Office of the President, *FY 2015 Annual Report to Congress: Federal Information Security Management Act* (Mar. 18, 2016), https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy_2015_fisma_report_to_congress_03_18_2016.pdf.

Table 2. Federal cybersecurity spending by agency (in millions) for FY2014[1250]

Agency	Prevent Malicious Cyber Activity	Detect, Analyze, and Mitigate Intrusions	Shaping the Cybersecurity Environment	Total
Department of Agriculture	$40	$46	$2	$88
Department of Commerce	$56	$83	$74	$213
Department of Education	$11	$20	$1	$32
Department of Energy	$108	$78	$71	$257
Department of Justice	$102	$433	$44	$579
Department of Labor	$13	$3	$1	$17
Department of State	$55	$54	$5	$114
Department of Transportation	$42	$44	$5	$91
Department of Veterans Affairs	$13	$131	$9	$153
Department of the Interior	$17	$30	$1	$48
Department of the Treasury	$122	$68	$10	$200
Department of Defense	$2,552	$1,225	$5,178	$8,955
Department of Health & Human Services	$54	$91	$25	$170
Department of Homeland Security	$473	$722	$148	$1,343
Department of Housing & Urban Development	$6	$8	$0	$14
Environmental Protection Agency	$1	$6	$0	$7
General Services Administration	$27	$16	$10	$53
International Assistance Programs	$9	$4	$3	$16
National Science Foundation	$3	$6	$154	$163
National Aeronautics & Space Administration	$35	$48	$19	$102
Nuclear Regulatory Commission	$4	$12	$3	$19
Office of Personnel Management	$2	$5	$0	$7
Small Business Administration	$1	$4	$0	$5
Social Security Administration	$46	$11	$2	$59
Total Cybersecurity Spending	**$3,792**	**$3,148**	**$5,765**	**$12,705**

NOTE: Due to rounding, categories may not sum to the total

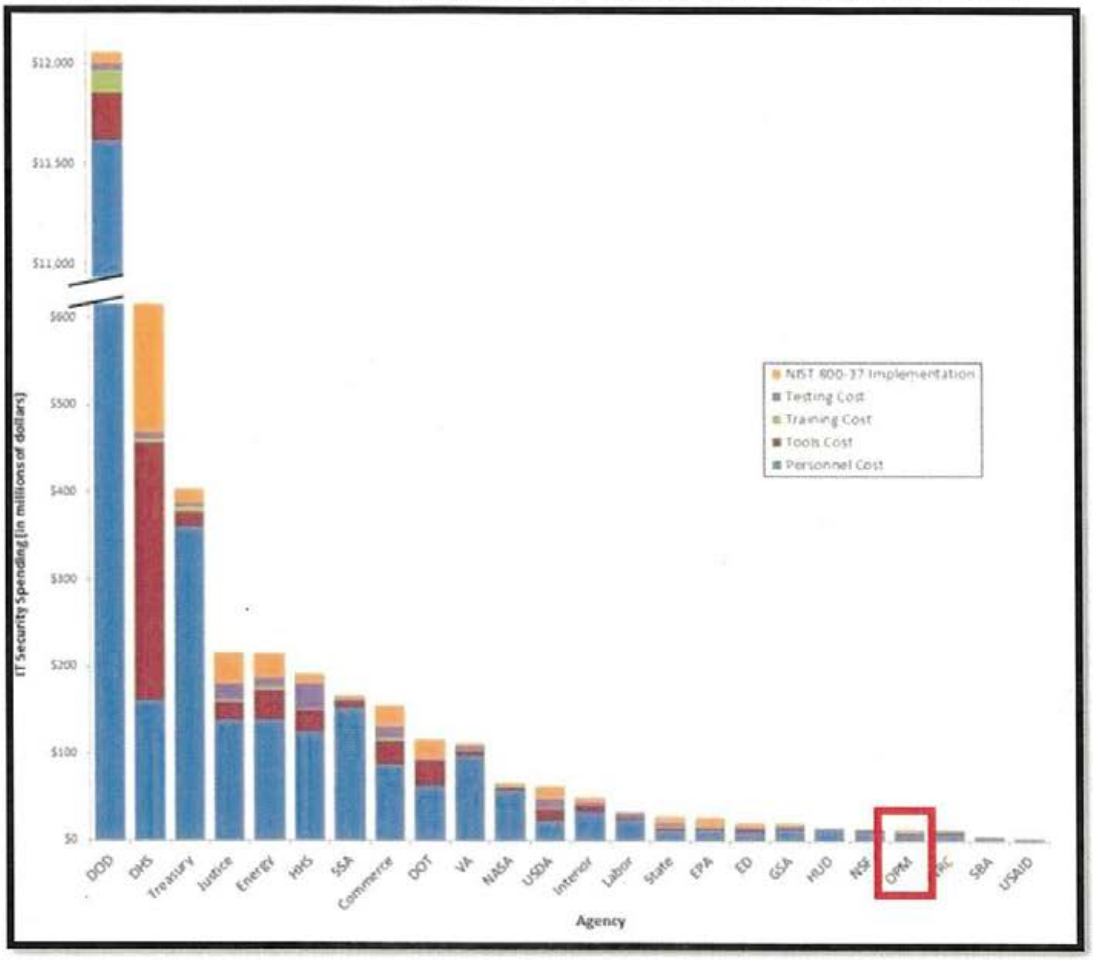
[1250] Office of Mgmt. & Budget, Exec. Office of the President, *FY 2014Annual Report to Congress: Federal Information Security Management Act* 83 (Feb. 27, 2015), https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy14_fisma_report_02_27_2015.pdf.

Table 3. Federal cybersecurity spending by agency (in millions) for FY2013[1251]

Agency	Prevent Malicious Cyber Activity	Detect, Analyze, and Mitigate Intrusions	Shape the Cybersecurity Environment	Total
Dept. of Agriculture	$39	$23	$1	$63
Dept. of Commerce	$47	$74	$42	$163
Dept. of Education	$11	$11	$0	$22
Dept. of Energy	$112	$69	$37	$218
Dept. of Justice	$105	$335	$6	$446
Dept. of Labor	$5	$9	$9	$23
Dept. of State	$51	$30	$5	$86
Dept. of Transportation	$44	$48	$5	$96
Dept. of Veterans Affairs	$11	$102	$7	$121
Dept. of the Interior	$13	$24	$1	$38
Dept. of the Treasury	$146	$109	$13	$268
Dept. of Defense	$2,471	$1,055	$3,580	$7,106
Dept. of Health & Human Services	$44	$111	$26	$181
Dept. of Homeland Security	$369	$590	$150	$1,109
Dept. of Housing & Urban Development	$4	$7	$0	$12
Environmental Protection Agency	$1	$19	$0	$20
General Services Administration	$28	$10	$8	$46
International Assistance Programs	$8	$7	$7	$22
National Science Foundation	$3	$6	$141	$150
NASA	$27	$40	$19	$86
Nuclear Regulatory Commission	$4	$10	$3	$17
Office of Personnel Management	$2	$5	$0	$7
Small Business Administration	$1	$4	$0	$5
Social Security Administration	$27	$11	$2	$40
Total Information Security Spending	**$3,575**	**$2,707**	**$4,063**	**$10,344**

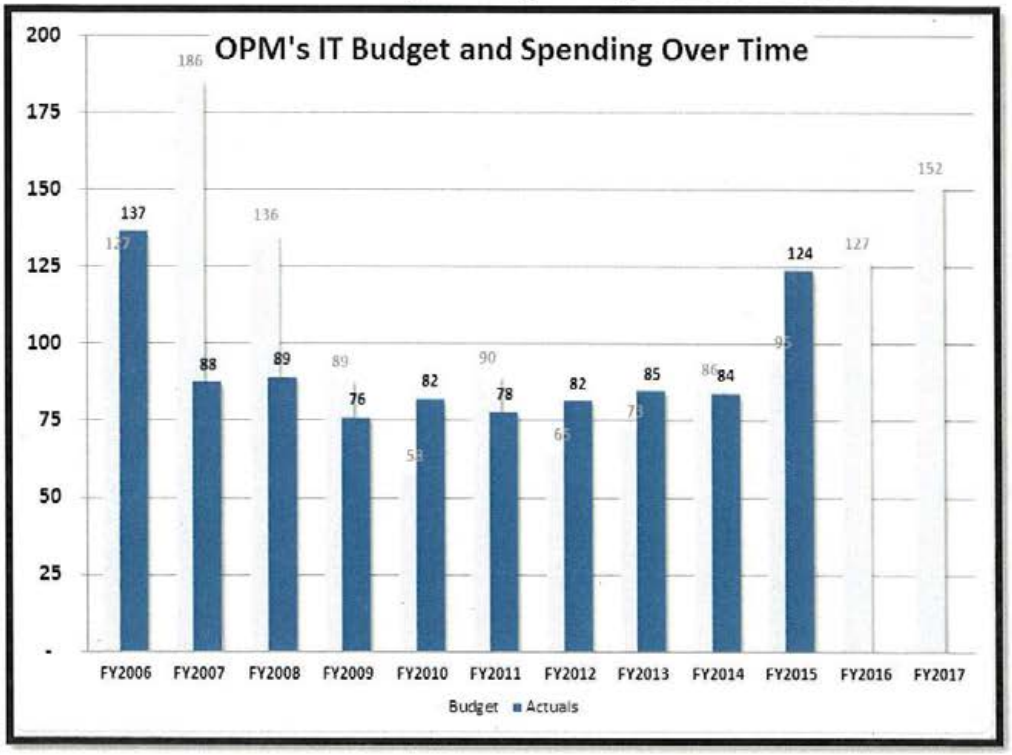
[1251] Office of Mgmt. & Budget, Exec. Office of the President, *FY 2013Annual Report to Congress: Federal Information Security Management Act* 65 (May 1, 2014), https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy_2013_fisma_report_05.01.2014.pdf.

Table 4. Federal cybersecurity spending by agency (in millions) for FY 2012[1252]



[1252] Office of Mgmt. & Budget, Exec. Office of the President, *Fiscal Year 2012 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002* (Mar. 2013), https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy12_fisma.pdf.

Table 5. OPM IT Budget and Spending, FY2006-FY2017[1253]



[1253] U.S. Office of Pers. Mgmt., *OPM Congressional Budget Justification Performance Budget FY2016*, at 2 (Feb. 2015), https://www.opm.gov/about-us/budget-performance/budgets/congressional-budget-justification-fy2016.pdf.. Cybersecurity is one line item in OPM's total IT budget. The amounts requested for IT spending overall, and the amounts appropriated, are shown in the Appendix. In addition, overall funding spikes in 2007 and 2008 are attributed to a transfer from the Trust Fund for retirement modernization. *See* U.S. Office of Pers. Mgmt., *OPM Congressional Budget Justification Performance Budget FY2007* (Feb. 6, 2006), https://www.opm.gov/about-us/budget-performance/budgets/2007-budget.pdf; U.S. Office of Pers. Mgmt., *OPM Congressional Budget Justification Performance Budget FY2008* (Feb. 5, 2007), https://www.opm.gov/about-us/budget-performance/budgets/2008-budget.pdf.