View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by UT Digital Repository

"SUCCESS IS INVISIBLE, BUT FAILURE IS PUBLIC"[1]: EXAMINING THE U.S. OFFICE OF PERSONNEL MANAGEMENT DATA RECORDS BREACH

Zeyi Lin

TC 660H
Plan II Honors Program
The University of Texas at Austin

May 10, 2018

_____

Prof. Robert M. Chesney
James A. Baker Chair and Associate Dean for Academic Affairs, School of Law
Director, Robert S. Strauss Center for International Security and Law
Supervising Professor

_____

Dr. William H. Press
Warren J. and Viola M. Raymer Chair
Department of Computer Science and Integrative Biology
Second Reader

[1] This phrase comes from Susan Hennessey, managing editor of the national security-focused online publication *Lawfare*, in a cybersecurity review essay published in the November/December issue of *Foreign Affairs*. In this essay, Hennessey contextualizes the 2015 cyberattack on the U.S. Office of Personnel Management (OPM) alongside the greater deterrence strategy of cyberspace with this quote. Indeed, success in cybersecurity is hard to appreciate until it is gone, usually in the most public of circumstances.

Acknowledgements

First, I would like to thank my family and friends for their love and support.

Next, I would like to thank my advisor, Prof. Bobby Chesney, and my second reader, Dr. Bill Press, who provided me with excellent guidance as I navigated through this thesis process. I would like to especially thank Prof. Chesney for instilling in me an academic interest in cybersecurity and policy. I am also very appreciative of Dr. Press, whose meticulous edits helped sharpen the language of this document.

Abstract

Author: Zeyi Lin

Title: "Success is Invisible, but Failure is Public": Examining the U.S. Office of Personnel Management Data Records Breach

Supervising Professor: Prof. Robert M. Chesney, The University of Texas School of Law and Robert S. Strauss Center for International Security and Law

In 2015, the U.S. Office of Personnel Management (OPM) suffered one of the largest government-related data breaches in U.S. history. A total of 4.2 million personnel records, 21.5 million background check records, and 5.6 million sets of fingerprints were exfiltrated in a sophisticated, multi-stage cyber espionage operation linked to state-sponsored actors. Such a large data breach invited bipartisan criticism of the agency's handling of the incidents and thrust the federal government's cybersecurity preparedness into the limelight.

This paper seeks to answer a set of five interrelated questions: 1) What happened in the 2015 U.S. Office of Personnel Management Data breach, and what were the impacts? 2) Did a lack of technical capability hinder OPM's efforts to detect and block unauthorized access to its network? 3) Were organizational and management weaknesses more to blame? 4) Did the cybersecurity posture at OPM before the incidents change after the events in 2014 and 2015? 5) What can be done by the Office of Personnel Management to prevent or mitigate the damage from similar cyber activities in the future?

To answer these questions, this paper first introduces the concept of the "cybersecurity toolkit" to better understand contemporary cyber issues. Second, the OPM case study is discussed, including a timeline of events and key actors. Third, this paper examines the technical, management, and compliance-related factors that contributed to the breaches, including a compilation and analysis of OPM Inspector General cybersecurity audit data from 2007 to 2017. Finally, this paper discusses the short- and long-term impacts of the OPM breach and offers recommendations to improve cybersecurity at OPM and within the federal government.

Table of Contents

Introduction

Imagine that you are an American citizen attempting to gain a security clearance for a national security position within the U.S. federal government. Integral to the application process of acquiring any security clearance to handle any classified information is the completion of Standard Form 86, or the SF-86. Beyond the cursory personally identifiable information and biographical details required by the SF-86, such as Social Security Number, U.S. passport information, citizenship, past addresses, among other, the form also asks for extremely sensitive details of your private life to minimize the risk of your compromise to foreign agents or governments. It asks for people who know you well; your marital status; and all of your foreign business, professional activities, and contacts. The SF-86 then digs deeper, asking about your psychological and emotional health, any illegal use of drugs or drug activity, and your financial record. When you complete the last page and send the SF-86 in, these details are then processed by the U.S. Office of Personnel Management (OPM), the federal agency that manages the U.S. government's civilian workforce. You, along with millions of others seeking positions of national security importance, trust this veritable list of immensely personal details in the hands of the federal government, for the immense potential personal, financial, and psychological damage caused if these personal details were to be leaked, stolen, altered, or otherwise breached, would be catastrophic.

Unfortunately, as OPM discovered in investigating a breach of its systems in June 2015, several million records were stolen by hackers in multiple incidents from as early as 2014. Such a heist was one of the largest made against the U.S. federal government in its history, and the failures leading up to the breach suggested that the OPM was caught off guard.[2] On June 4,

[2] U.S. Library of Congress, Congressional Research Service, *Cyber Intrusion into U.S. Office of Personnel Management: In Brief*, by Kristin Finklea, Michelle D. Christensen, Eric A. Fischer, Susan V. Lawrence, and Catherine A. Theohary. R44111, July 17, 2015, https://fas.org/sgp/crs/natsec/R44111.pdf, 1.

2015, OPM announced that the personnel data of approximately 4.2 million current and former federal employees were compromised in a cyber incident discovered earlier that year and offered to provide "credit report access, credit monitoring, and identity theft insurance and recovery services to potentially affected individuals" for the following 18 months.[3] Five days later, OPM announced that an incident from late May, 2015, resulted in a breach of the sensitive background investigation information of 21.5 million individuals, including Social Security Numbers, residency and education history, employment history, criminal, and financial history, among many other highly sensitive personal details.[4] Of the 21.5 million records stolen, 19.7 million records contained data of "current, former, and prospective employees and contractors *who applied for a background investigation* in 2000 and after."[5] The other 1.8 million records were of non-applicants "married or otherwise cohabitating with background investigation applications."[6] Furthermore, OPM later confirmed the loss of 5.6 million fingerprint records.

Malicious cyber activities against OPM date as far back as March 2014, when a contractor for OPM handling U.S. security clearance background clearances was allegedly breached by Chinese hackers.[7] Just three months later, in July, 2014, OPM networks containing information of applicants for Top Secret clearances were breached. The sheer volume of data loss by the government agency handling federal employee personnel data, background check records, and other personally identifiable information raises several questions about how

---

[3] U.S. Office of Personnel Management, "OPM to Notify Employees of Cybersecurity Incident," *OPM.gov*, June 4, 2015, https://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident/.
[4] U.S. Office of Personnel Management. Office of Communications, "OPM Announces Steps to Protect Federal Workers and Others from Cyber Threats," *OPM.gov*, June 9, 2015, https://www.opm.gov/news/releases/2015/07/opm-announces-steps-to-protect-federal-workers-and-others-from-cyber-threats/.
[5] U.S. Library of Congress, Congressional Research Service, *OPM Data Breach: Personnel Security Background Investigation Data,* by Michelle D. Christensen, IN10327, July 24, 2015, https://fas.org/sgp/crs/natsec/IN10327.pdf.
[6] Cyber Intrusion into U.S. Office of Personnel Management: In Brief, 2.
[7] "Significant Cyber Incidents," *Center for Strategic and International Studies*, 2018, https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity.

cybersecurity was prioritized within the U.S. Office of Personnel Management before these incidents, how the breaches were dealt with by OPM leadership and rank-and-file, and whether the impacts of an incident as large in scale as the OPM breach were enough impetus to change the cybersecurity posture of the Office of Personnel Management in the future.

Thesis Questions and Scope

This thesis examines the events leading up to the OPM data breaches and the handling of the repercussions that followed. Specifically, it will evaluate this timeline of events based on three guiding questions: 1) What happened in the 2015 U.S. Office of Personnel Management Data breach, and what were the impacts? Given the political firestorm that later erupted from Congressional oversight authorities, considering an object reconstruction of events is crucial. Evaluating both the short-term and long-term impacts of the OPM breaches would ground the discussion in a more actionable context for policymakers. 2) Did a lack of technical capability hinder OPM's efforts to detect and block unauthorized access to its network? In understanding any cybersecurity incident, it is necessary to consider the technical factors at play. 3) Were organizational and management weaknesses more to blame? No matter how strong or weak technical capabilities are in an organization, there are many human and management factors that affect the confidentiality, integrity, and availability of information assets in a network.

This thesis will then examine the timeline of events in context. Another important question involves the historical consideration of information security within the Office of Personnel Management: 4) did the cybersecurity posture at OPM before the incidents change after the events in 2014 and 2015? Analyzing OPM's compliance with relevant federal cybersecurity standards before and after the incidents offers a start. Finally, after facing much criticism from government oversight groups and public scrutiny over the incidents, 5) what can

be done by the Office of Personnel Management to prevent or mitigate the damage from similar cyber activities in the future?

The scope of this thesis covers the events leading up to, during, and immediately after the Office of Personnel Management data breaches. Current events and developments in U.S. federal government thinking on cybersecurity are provided when relevant. This thesis also analyzes historical Federal Information Security Management/Modernization Act (FISMA) compliance data of the Office of Personnel Management from 2007 to 2017 published by the OPM Office of the Inspector General. The cybersecurity efforts of other federal agencies are left as opportunities for further inquiry; a collective analysis of organization compliance may yield additional insights on the state of federal cybersecurity posture as a whole.

Methodology

To answer the questions posed above, this thesis first provides a theoretical foundation of the modern cybersecurity "toolkit," including definitions, categorizations, and institutions committed to cybersecurity work. An explanation of the relevant actors involved with cybersecurity in the U.S. federal government sets the scene for the OPM breach. Sources relating to building this theoretical foundation include recently published books that incorporate contemporary cybersecurity theory into relevant case studies and documents that outline the structure of how cybersecurity efforts are organized within the U.S. federal government.

Second, this thesis will reconstruct a timeline of the breach based on a fact base of government reports, news articles, and technical analyses. The timeline of events draws from the two detailed reports published by the House Committee on Oversight and Government Reform in 2016: a report entitled "The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation" by the Republican majority staff, under Chairman Jason Chaffetz of Utah, and responding memo to the Democratic staff on the

committee, authored by Ranking Minority Member Elijah E. Cummings of Maryland. Contemporaneous news sources, from both mainstream media and more technically-focused publications, supplement the timeline of events with additional detail. Furthermore, technical analyses, particularly attribution reports, are used in order to answer questions regarding OPM's technical capabilities in defending itself against the incidents.

Finally, a dataset of Office of Personnel Management FISMA (Federal Information Security Modernization Act) annual audit reports from 2007 to 2017, authored by the OPM Office of the Inspector General (OIG), was collected and mined to analyze the longer-term cybersecurity preparedness of OPM. Three important aspect of these audit reports were problem findings, the recommendations offered by the OIG, and the history of each recommendation, including whether it was rolled-forward from a previous report (and if so, what the history of each roll-forward can tell about the type of policy recommendation made). Looking at the data several years before the OPM breaches occurred offers a historical perspective of cybersecurity posture at the agency. If data were available regarding the implementation status of each recommendation made by the OPM OIG, then such data were included in the dataset. If data on recommendation closure was not explicitly available (i.e., a specific year's OIG report redacted certain implementation progress markers) and a recommendation was not determined to be open in the following year, the closure date of the recommendation was assumed to be the date of the corresponding OIG report's release. Furthermore, the age of all open recommendations is calculated from the initial issuance of the recommendation up until March 30, 2018. Typically, the OIG releases semiannual reports to Congress on the 30th day of September or March of each year. However, as of May 1, 2018, a report on "Open Recommendations as of March 30, 2018" has not been released. The March 30, 2018 date was selected because it is next the semiannual report milestone after the currently

published "Open Recommendations as of September 30, 2017" report to Congress and allows for better approximation of the age of recommendations.[8]

Comparing and contrasting the FISMA compliance in the years immediately before the incidents and the reports post-breaches approximates a measure cybersecurity posture within the agency. A wider comparison of security posture and FISMA compliance across federal agencies is an area left for further research. While the general approach taken in this thesis may be applicable and aggregable for other federal agencies, OPM remains the focus as the added scrutiny and government investigative work following the OPM breaches draw attention to the agency's cybersecurity troubles as a unique case.

[8] David Kennel, "OPM vs. APT: How Proper Implementation of Key Controls Could Have Prevented a Disaster," *SANS Institute*, March 10, 2016, https://www.sans.org/reading-room/whitepapers/breaches/opm-vs-apt-proper-implementation-key-controls-prevented-disaster-36852, 8.

Part One: The Cybersecurity Toolkit

For governments, developments in information technology have yielded tangible benefits in domestic policymaking, intelligence gathering, military action, and beyond. Amidst major cybersecurity incidents in both the public and private sectors, former President Barack Obama called cyberspace the "wild West."[9] The 2015 U.S. Office of Personnel Management breach was "one of the largest reported on federal government systems"[10] and "shocked the U.S. government,"[11] but not the only serious cyber intrusion against federal systems in recent memory. In the two years prior to the OPM breach, foreign cyber actors were able to penetrate the networks of the State Department, Pentagon, and White House.[12] Non-state cyber intruders have also had success on U.S. government systems, including gaining access to the personal email accounts of the Director of the Central Intelligence Agency and the Director of National Intelligence in 2015 and 2016.[13] This chapter will briefly discuss several background issues to better the reader's understanding of the "cybersecurity toolkit": (1) different views on and the segmentation of cybersecurity, including the defensive lens through which this thesis examines the OPM breach; (2) the concept of the "cybersecurity dilemma" in international relations and how it pertains to the 2015 OPM incident; and (3) the current landscape of U.S. cybersecurity institutions and where the OPM sits within it.

[9] Bill Chappell, "Obama: Cyberspace Is the New 'Wild West,'" *NPR*, February 13, 2015, https://www.npr.org/sections/thetwo-way/2015/02/13/385960693/obama-to-urge-companies-to-share-data-on-cyber-threats.
[10] *Cyber Intrusion into U.S. Office of Personnel Management: In Brief*, 1.
[11] Brendan I. Koerner, "Inside the Cyberattack that Shocked the US Government," *Wired*, October 23, 2016, https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/.
[12] Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations* (New York: Oxford University Press, 2016), 160.
[13] Ibid., 161.

1.1. Different Views of Cybersecurity

Cybersecurity is a broad term that encompasses protecting information and communications technology (ICT) systems and their contents from cyberattacks, focusing on the concepts of information confidentiality, integrity, and availability. Cybersecurity "is also sometimes conflated inappropriately in public discussion with other concepts such as privacy, information sharing, intelligence gathering, and surveillance."[14] Cybersecurity has important implications for these other concepts, however. For example, good cybersecurity may protect the privacy of individuals or organizations, such as the personally identifiable information of millions of the current and former government employees lost in the OPM breach. Inter-organization and intra-organization information sharing may bolster the cybersecurity capabilities, but that information may include personal details. Cybersecurity may be useful in protecting from intelligence gather efforts by an adversary, but the defender might also gather intelligence on potential adversaries to bolster its cybersecurity.

The risks of cyberattack are functions of several factors: threats, vulnerabilities, and impacts. Cyber threats are the actors who are carrying out cyberattacks, ranging from criminals, spies, nation-state warriors, "hacktivists," and terrorists. Vulnerabilities are weaknesses or oversights in ICT system design or flaws in the implementation of a system.[15] Malicious actors may target certain vulnerabilities using exploit code to gain unauthorized access to a system, and then utilize further malicious code to deploy within the system.[16] Cyberattacks "can compromise the confidentiality, integrity, and availability of an ICT system and the information it handles."[17] In particular, cyberattacks on components of critical infrastructure (CI), including

[14] U.S. Library of Congress, Congressional Research Service, *Cybersecurity Issues and Challenges: In Brief*, by Eric A. Fischer, R43831, August 12, 2016, https://fas.org/sgp/crs/misc/R43831.pdf.
[15] Ibid, 2.
[16] Buchanan, 35.
[17] *Cybersecurity Issues and Challenges: In Brief*, 2.

physical infrastructure, such as water, power, sewage and refineries, as well as economic infrastructure, such as stock exchanges, banks, and credit card networks, could have could have significant effects on national security, the economy, and the livelihood and safety of individual citizens.[18] The OPM breach is a case in which nation-state spies or warriors exploited a series of vulnerabilities in OPM's network infrastructure and gained unauthorized access to its systems, compromising the confidentiality of millions of data records. As a means of understanding the risks and impacts of malicious cyber activities and exploring the OPM breach in more detail, cybersecurity can be segmented in several ways. The rest of this section discusses the offensive versus defensive elements of cybersecurity, public sector versus private sector efforts in cybersecurity, and introduces the analysis of the OPM from the defensive cybersecurity perspective.

1.1.1 Offensive versus Defensive Elements

Strategically, cyber operations exist along a spectrum: they can be benign or aggressive, passive or active.[19] Tactically, offensive action taken in cyberspace means breaking into another computer network. The process of breaking into a computer network comprises a multi-step intrusion model: target acquisition, development, authorization, entry, command and control, pivoting, payload activation, and confirmation.[20] From a defender's perspective, a baseline network defense model involves preparation, detection, data collection, analysis, containment, and decontamination.[21] Both offensive and defensive cyber actions are situated within the cybersecurity and foreign policy toolkit that nations deploy. Analyzing the 2015 OPM data breach from the intruder's perspective enables a greater understanding of the vulnerabilities

[18] *Cybersecurity Issues and Challenges: In Brief*, 2.
[19] Matteo G. Martemucci, "Offensive Dimensions of Cyber Security: Strategy and Policy Challenges," *U.S. Air Force 318th Cyberspace Operations Group*, August 2014.
[20] Buchanan, 33.
[21] Ibid., 53.

exploited by attackers in the OPM network. Examining the incident from a defensive perspective provides insight into both the technical ability of OPM to defend against digital attacks, and the human dimension of OPM. The defensive angle, then, is particularly useful when determining longer-term policy recommendations to prevent or mitigate intruders from successfully deploying attacks of this scale.

1.1.2 Public Sector versus Private Sector Efforts

In the public sector, or government model, minimizing cyber risk is a priority that must be done at the expense of efficiency. An intelligence agency, for example, must balance between (i) fostering informed public debate and motivating the public into action by disclosing vulnerabilities, versus (ii), keeping closely-held, actionable information on an adversary outside of the public domain to guard an information advantage. In the private sector, the business model for managing risk serves an underlying profit motive. Customers' perception of security and stability of a business' brand may dis-incentivize executives from disclosing cyber risks.[22] Thus, there are fundamentally different approaches between how the public sector and private sectors can combat cyber intrusions.[23] The U.S. government has the full force of the law behind it to respond to cyber incidents, whether through intelligence gathering, containment, or pursue even more aggressive cyber action. Under current U.S. law, however, defensive intrusions, or "hack back," by private citizens and corporations are illegal. If allowed, there are risks of online vigilantism and greater cyber-instability.

1.2. The Cybersecurity Dilemma

In traditional international relations theory, the security dilemma refers to the oftentimes counterintuitive notion that, given an anarchic international system, "many of the means by

[22] Martemucci.
[23] Ibid.

which a state tries to increase its security decrease the security of others."[24] Recent theorists have broken down the security dilemma into two sequential parts: one is the dilemma of interpretation, in which a state attempts to ascertain the intent of another state's actions, commonly under conditions of incomplete information; the other is the dilemma of response, in which decision-makers must choose from a spectrum of options that each have consequences of varying severity.[25] The actions of one nation may inadvertently provoke further brinksmanship from the nation being surveilled, and escalate towards real conflict.

While decision-makers in international relations often grapple with situations of incomplete information, the problem of information asymmetry is far more severe in cyberspace. Attribution, which involves identifying an actor and identifying that actor's motivations behind orchestrating a cyber incident, is much more difficult. Accurate attribution allows the target of a cyber intrusion (such as the United States government) to determine the best mechanism for response, ranging from law enforcement measures to diplomatic or military tools.[26] Meanwhile, determining the intent of a state's cyber activities is even more complicated, as almost all actions may be seen as offensive and existentially threatening to the networks, devices, or people of another state. Thus, "there is only a nascent status quo" in cybersecurity.[27]

Given that "computer hacking is now part of international relations" and part of the "tools of statecraft,"[28] situating the 2015 Office of Personnel Management data breach within the cybersecurity dilemma allows for better understanding of both the motives behind the hack and the reasoning for OPM's response. Clearly distinguishing between the offensive and defensive

[24] Robert Jervis, "Cooperation Under the Security Dilemma," *World Politics* 30, no. 2 (January 1978): 169.
[25] Buchanan, 20.
[26] *Cyber Intrusion into U.S. Office of Personnel Management: In Brief*, 2.
[27] Buchanan, 8.
[28] Ibid., 9.

elements of cybersecurity reveals different strategic implications and offers insight into policymaking to suit both needs.

1.2.1 OPM Breach Attribution in the Nascent Status Quo

Cyber activity attribution is a multi-faceted process with different implications for decision-makers. It "draws on all sources of information available, including technical forensics, human intelligence, signals intelligence, history, and geopolitics, among others."[29] In recent years, attribution capabilities have strengthened because more nations are attentive to the risks of malicious cyber activity and have invested more attention and resources into the issue. Improved data collection over the course of a decade has yielded a better "historical corpus," and both the tools and analysts tasked with looking at the data are more seasoned. Dedication of attention and resources is a long-term investment as these nations strengthen their attribution capabilities.[30] On the other hand, as potential cyber adversaries grow more skilled, they are more aware that they are being tracked for attribution purposes. They can plant false clues or flags, deny activities outright, or discredit circumstantial evidence, to avoid being discovered and to discredit attribution overall. Attribution of the OPM breach had important international relations ramifications for the United States, particularly with China. Immediately after news of the OPM breach broke out, the official U.S. government stance shied away from specific attribution of the incident to any actor. But within the same month, former Director of National Intelligence James Clapper named China as the "leading suspect" behind the OPM attacks and "expressed grudging admiration" for the alleged Chinese hackers.[31]

[29] Herbert Lin, "Attribution of Malicious Cyber Incidents: From Soup to Nuts," *Hoover Institution Aegis Paper Series,* no. 1607, September 19, 2016, https://www.hoover.org/sites/default/files/research/docs/lin_webready.pdf.
[30] Lin, 45.
[31] *Cyber Intrusion into U.S. Office of Personnel Management: In Brief*, 2.

1.2.2 The Cybersecurity Dilemma: Taking the Defensive Perspective

Given the persistence of cyber adversaries and their efforts against ICT systems in general, and not just OPM's networks, there are clear needs for a network architecture that can resist existing and novel attacks, collect actionable intelligence on potential intruders, and enable clever defenders to act decisively on that information. A proposed model of baseline network defenses includes the six concepts of preparation, detection, data collection, analysis, containment, and decontamination. Some scholars, such as Ben Buchanan, argue that multiple, asynchronous failures across many different elements and levels within in the OPM's defensive model are what caused the breach to happen. Within the context of the cybersecurity dilemma, "states have great incentive to penetrate the networks and operations of other states, even before they are themselves targeted."[32]

In the defensive model, preparation involves reducing the attack surface (the reachable and exploitable vulnerabilities in a network) by network administrators, on the "defender's turf."[33] Minimizing the attack surface can be achieved by applying regular patches, testing updates, and monitoring user accounts. However, software patches are complex in large organizations and especially complex for critical infrastructure operators, meaning that at any given time, there are likely to be machines running outdated software that contain vulnerabilities for intruders to exploit. Defenders often do not have great knowledge of their own network; better understanding the topology of and reducing the number of entry and exit points to the network enables easier spotting of deviations from a normal, secure baseline.

Preparation is especially important for the detection of a cyber intrusion or cyberattack. Detection may be external, in which a third-party organization informs the victim of an

[32] Buchanan, 64.
[33] Ibid., 54.

intrusion of the malicious activity, or internal, in which a victim's own defensive team may uncover evidence of intrusion. Most (approximately 90 percent) cyber intrusions are detected externally, and the rest internally.[34] Defensive teams may uncover evidence of and detect intrusions using pattern-matching or signature-based detection against the code, techniques, and infrastructures of known intruders. There are three different indicators of compromise, including atomic indicators, computer indicators, and behavioral indicators, that teams may use for detection. They can also use pattern-matching tools to compare known indicators of malicious cyber activity with activity inside their own networks. Defenders may specifically employ "hunters," analysts who look proactively for weaknesses within the network and malicious code that may exploit those weaknesses. Detection is a challenge whose difficulty enormously benefits intruders by giving them more time to exploit and attack within the network, but improving detection is a "key part of strengthening overall network defense."[35]

Once an intrusion into an ICT system is detected, further data collection and analysis are concurrent processes that provide more information about the exploited vulnerability and the attacker. Data collection informs analysis, and vice versa.[36] Defenders must work quickly to analyze the information on which computers and accounts on their networks intruders have compromised, potentially reconstructing events and deconstructing malicious code to better understand how it works. At this point, intruders may mislead defenders using specific functionalities within their malicious code, making data collection and analysis a time-consuming step and underscoring the need for proper preparation and ample internal network visibility on the part of the defenders in the case of an intrusion.

[34] Buchanan, 56.
[35] Ibid., 59.
[36] Ibid., 61.

With enough information on the intruder, it is ultimately up to the decision-maker to choose the best method to contain the attack. The defender may directly interfere with the operations of intruders, e.g., by identifying the command and control mechanism of the intrusion to block it or observe commands; setting up "honeypots" to distract attackers; or blocking intruders' actions after malware deployment to prevent exfiltration. Defenders must be aware of techniques used by skilled intruders to make containment difficult, such as encryption, unconventional exit routes, and compromised machines.[37]

Once an intrusion or attack is contained, decontamination follows.[38] Defenders can immediately discard computer hardware entirely to rid the network of a potential recurring vector of attack. Or they can use human investigators and automated tools to lead deep and intense scans of their network for any remaining signs of malicious code or anomalous activity. Besides these immediate actions, defenders must also adapt to a cyber incident and be able to stop the next operation. They may be able to deploy more automated tools for detection or collect better intelligence from those tools. Organizational changes may also result and require a lengthy approval and implementation process but is essential to effecting better cybersecurity. The defenders then return to the preparation step, starting the cycle over again.

1.3 Contextualizing Cybersecurity in the U.S. Federal Government

The United States government's cyber incident response structures encompass a whole-of-government approach. Federal law across more than 50 statutes task all federal agencies with cybersecurity responsibilities for their own systems as well as critical infrastructure-specific responsibilities.[39] In general, the Office of Management and Budget (OMB) oversees the

[37] Buchanan, 62.
[38] Ibid., 63
[39] *Cyber Intrusion into U.S. Office of Personnel Management: In Brief*, 3.

implementation of cybersecurity standards developed by the National Institute of Standards and Technology (NIST) in federal civilian ICT systems, under the Federal Information Security Modernization Act (FISMA), originally the 2002 Federal Information Security Management Act and later updated in 2014 by the U.S. Congress.[40]

1.3.1. The Federal Information Security Modernization Act of 2014

FISMA as it stands today reestablishes the oversight authority of the Director of the OMB and the Secretary of the Department of Homeland Security (DHS) to secure civilian government information systems. FISMA directs agency heads "to ensure that: (1) information security management processes are integrated with budgetary planning; (2) senior agency officials, including chief information officers, carry out their information security responsibilities; and (3) all personnel are held accountable for complying with the agency-wide information security program."[41] Furthermore, it calls for the use of automated tools in periodic agency risk assessments, security testing, and incident detection, reporting, and response. The 2014 FISMA update also calls for agencies to give timely notification of major information security incidents to Congress (within a week) and directs agencies to submit annual reports regarding information security preparedness, including "(1) threats and threat actors, vulnerabilities, and impacts; (2) risk assessments of affected systems before, and the status of compliance of the systems at the time of, major incidents; (3) detection, response, and remediation actions; (4) the total number of incidents; and (5) a description of the number of individuals affected by, and the information exposed by, major incidents involving a breach of personally identifiable information."[42]

---

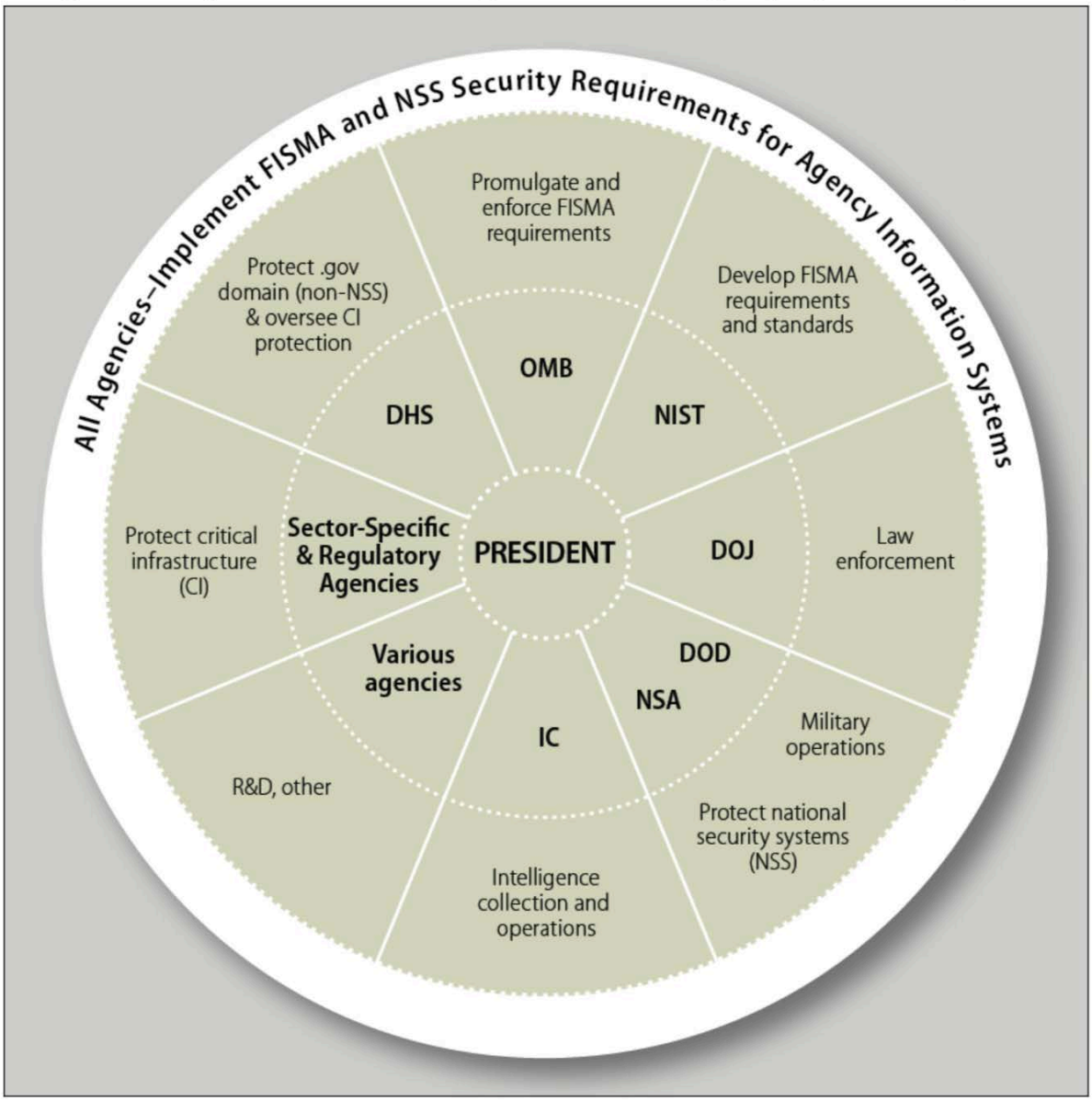
[40] *Federal Information Security Modernization Act of 2014*, Public Law 113-283, 128 Stat. 3073-3088, December 18, 2014, https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf.
[41] *Federal Information Security Modernization Act of 2014.*
[42] Ibid.

1.3.2. Cybersecurity in the Rest of the U.S. Government

Military ICT systems fall under the purview of the Department of Defense (DOD).[43] Through the National Security Agency (NSA), the DOD is also responsible for the security of national security systems (NSS). The Department of Homeland Security (DHS) has operational responsibility to protect federal civilian systems and private sector critical infrastructure when they are under cyber threat.[44] DHS also coordinates federal information sharing between civilian systems through the National Cybersecurity and Communications Integration Center (NCCIC). The Department of Justice (DOJ) leads federal cyber law-enforcement efforts.[45] A diagram of various federal agency cybersecurity roles highlighting interagency relationships is provided below.[46]

[43] *Cybersecurity Issues and Challenges: In Brief*, 3.
[44] Ibid.
[45] Ibid.
[46] Ibid., 4.

Figure 1. Simplified Schematic Diagram of Federal Agency Cybersecurity Roles



Source: CRS.

Notes: DHS: Department of Homeland Security; DOD: Department of Defense; DOJ: Department of Justice; FISMA: Federal Information Security Management Act; IC: Intelligence Community; NIST: National Institute of Standards and Technology; NSA: National Security Agency; OMB: Office of Management and Budget; R&D: Research and development.

Figure 1. U.S. Federal Government Cybersecurity Relationships and Infrastructure

Both federal agencies and the legislative branch have increasingly focused on cybersecurity in recent years. A significant portion--roughly one in every seven dollars--of agency IT budgets constitute funding for cybersecurity, with the FISMA proportion of total IT

spending in 2015 at nearly double the amount spent in 2006.[47] Legislation proposed in the 111th and enacted in the 113th and 114th sessions of Congress have centered on cybercrime laws, data-breach notification, FISMA reform, information sharing, addressing issues in the "Internet of Things," improving privately-held critical infrastructure, updating research and development, and improving the "size, skills, and preparation" of the cybersecurity workforce.[48] Despite a strong emphasis on cybersecurity efforts within the federal government, that OPM was a victim of two major data breaches in 2015 suggests that there is still much more work to be done.

[47] *Cybersecurity Issues and Challenges: In Brief*, 3.
[48] Ibid., 5-6.

Part Two: The OPM Case Study

The basics of the cybersecurity toolkit offered in Part One allows for deeper examination of the Office of Personnel Management case study. The defensive perspective is particularly useful when it comes to triaging the underlying issues in the OPM data breaches, whether they are technical weaknesses, management failures, or a combination of the two. Applying some of the concepts from Part One's toolkit, this chapter (1) offers background about the U.S. Office of Personnel Management; (2) provides a detailed timeline of events about the OPM data breaches; and (3) introduces and examines the relationships between the key actors involved

2.1. About the U.S. Office of Personnel Management

2.1.1. The Mission of OPM

Founded on January 1, 1979, by the Civil Service Reform Act of 1978,[49] the U.S. Office of Personnel Management (OPM) replaced the former U.S. Civil Service Commission.[50] OPM is a federal agency that "serves as the chief human resources agency and personnel policy manager" for the U.S. government.[51] OPM serves a three-pronged mission: human capital management, benefits, and vetting. First, as part of human capital management, OPM designs, develops, and promulgates government-wide human resources systems as well as technical guidance for human resources management policies and practices. To build a "high quality public sector workforce," OPM works with other government agencies and "provides agencies with access to pre-competed private contractors."[52] OPM also provides oversight of best practices in the federal civil service.

---

[49] *Civil Service Reform Act of 1978, 5 U.S. Code 1101,* Public Law 95-454, 92 Stat. 1119-1227, October 13, 1978, https://www.gpo.gov/fdsys/pkg/STATUTE-92/pdf/STATUTE-92-Pg1111.pdf.
[50] Ibid., 92 Stat. 1183.
[51] U.S. Office of Personnel Management, "About Us," *OPM.gov,* https://www.opm.gov/about-us/.
[52] U.S. Office of Personnel Management, "What We Do," *OPM.gov*, https://www.opm.gov/about-us/our-mission-role-history/what-we-do/.

Second, OPM administers benefits for federal employees and their families, including insurance benefits for "more than eight million federal employees, retirees, and their families" and the Federal Retirement Program for "more than 2.7 million active employees" and "nearly 2.6 million annuitants, survivors, and family members."[53] In total, OPM handles the benefits of roughly 13 million people annually. A data breach of the systems involved in processing those benefits would pose a significant risk to those individuals.

Third, OPM and its contractors vet prospective employees in the federal hiring process. The most important function that OPM serves is performing background checks for security clearances for government employees and contractors.[54] These background checks include standard OPM forms such SF 85 (Questionnaire for Non-Sensitive Positions) and the SF 86 (Questionnaire for National Security Positions).[55] To complete an SF 86 (and be eligible for a clearance to handle classified information in a national security position), an applicant must fill out personally identifiable information including about relatives, spouses, mental health, finances, among many other sensitive topics.[56] Implicit in the third prong of OPM's mission is protecting information collected and processed in the vetting process for federal employment.

2.1.2. OPM Leadership and Organizational Structure

The Director of the Office of Personnel Management leads the agency. Since OPM's creation in January 1979, there have been 11 permanent Directors appointed by the President and confirmed by the Senate.[57] Katherine Archuleta (appointed in May 2013) was the

[53] U.S. Office of Personnel Management, "What We Do."
[54] Ibid.
[55] U.S. Office of Personnel Management, "Standard Forms," *OPM.gov*, https://www.opm.gov/forms/standard-forms/.
[56] U.S. Office of Personnel Management, "Questionnaire for National Security Positions," Standard Form 86, OMB No. 3206 0005, *OPM.gov,* Revised December 2010, https://www.opm.gov/forms/pdf_fill/sf86-non508.pdf.
[57] U.S. Office of Personnel Management, "Our Mission, Role & History," *OPM.gov,* https://www.opm.gov/about-us/our-mission-role-history/agency-leadership/.

permanent Director presiding over OPM during the data breaches and resigned on July 10, 2015. After Archuleta's resignation two Acting Directors led the agency before a permanent replacement could be found. The first, Beth Cobert, was in office from July 10, 2015 to January 19, 2017.[58] The second, Kathleen McGettigan, served from January 19, 2017 to March 9, 2018.[59] On March 9, 2018, Jeff T. H. Pon was confirmed as the 11th permanent Director of the Office of Personnel Management, after nearly three years without a permanent director.[60]

The Office of the Director manages five different vertical functions within OPM: 1) various Program Divisions; 2) the Office of the General Counsel; 3) Office of Communications; 4) Congressional, Legislative and Intergovernmental Affairs; and 5) various Support Functions.[61] First, OPM program divisions focus on federal government human resources management, including employee services, retirement services, healthcare and insurance, merit system accountability and compliance, suitability executive agent, the National Background Investigations Bureau, and other human resources solutions. Second, the Office of the General Counsel offers legal advice and representation for OPM leadership and also plays an enforcement and arbitration role related to federal government employee practices. Third, the Office of Communications informs the broader public about OPM's work. Fourth, Congressional, Legislative, and Intergovernmental Affairs is the chief conduit between OPM and the U.S. Congress, with Congressional relations, legislative analysis, constituent services, and intergovernmental affairs functions. Fifth, OPM's support function offices include the Chief

[58] Eric Katz, "With No Confirmed Director, OPM Could Struggle to Implement Trump's Agenda," *Government Executive*, August 17, 2017, https://www.govexec.com/management/2017/08/no-confirmed-director-opm-could-struggle-implement-trumps-agenda/140332/.
[59] See section on Kathleen McGettigan in U.S. Office of Personnel Management, "Our People & Organization: Senior Staff Bios," *OPM.gov*, https://www.opm.gov/about-us/our-people-organization/senior-staff-bios/.
[60] Ibid. See section on Jeff T. H. Pon.
[61] See the sidebar of the following URL: https://www.opm.gov/about-us/our-people-organization/office-of-the-director/.

Financial Officer, the Chief Information Officer, Planning and Policy Analysis, Diversity and Inclusion, Equal Employment Opportunity, Facilities, Security, and Emergency Management, and the Federal Prevailing Rate Advisory Committee. Independent of the Director's office is the Office of the Inspector General (OIG), which is an internal watchdog group that conducts audits of key OPM programs and provides recommendations to improve OPM's performance.[62] Under OIG are the Office of Legal and Legislative Affairs, the Office of Audits, the Office of Investigations, the Office of Evaluations and Inspections, and the Office of Management. An organizational chart summarizing the OPM's leadership structure is provided in Appendix I.

2.1.3. Information Technology Systems Architecture at OPM

Publicly available specifications of OPM's information technology systems architecture are largely contained within the OPM's Inspector General (OIG) annual FISMA audits. As of 2017, OPM's system inventory indicated that the agency's information technology network consisted of 46 major systems. [63] According to OPM's 2016 FISMA audit, 16 (over one-third) of those systems were operated by a contractor, with 82 interconnections those systems with agency-operated systems. The Federal Information Security Modernization Act of 2014 requires all federal agencies to monitor and test security controls, develop and test contingency plans, use the plan of action and milestones process, among other requirements. For instance, in 2015, the year of the major OPM breach, the OIG found that a total of 30 systems were subject to annual security control testing (20 of 29 systems operated by OPM, and 10 of 17 systems operated by a contractor).[64] Although OPM's performance in 2015 was lackluster, it worsened

[62] U.S. Office of Personnel Management, "Our Inspector General," *OPM.gov*, https://www.opm.gov/about-us/our-inspector-general/.
[63] U.S. Office of Personnel Management, Office of the Inspector General, Office of Audits, "Federal Information Security Modernization Act Audit Fiscal Year 2017," 4A-CI-00-17-020, October 27, 2017, 46.
[64] U.S. Office of Personnel Management, Office of the Inspector General, Office of Audits, "Federal Information Security Modernization Act Audit FY 2015," 4A-CI-00-15-011, November 10, 2015, 13.

significantly in 2017: only 9 of OPM's 46 systems were subject to adequate security controls testing and monitoring.[65]

2.2. Timeline of Events

The OPM breach occurred over a 12-month period and actually consisted of two distinct incidents in which OPM's networks were compromised: the first was reported in March 2014, and the second identified in April 2015. The timeline for these two attackers becomes muddled at times, as the House Oversight and Government Report Committee writes in its 2016 report that "sloppy cyber hygiene and inadequate security technologies… left OPM with reduced visibility into the traffic on its systems."[66] Furthermore, there was significant partisan disagreement in Congress over certain details of the breach timeline. The following timeline of events attempts to integrate the investigative findings from the House Committee report, drafted by Republican staff members under then-Chairman Jason Chaffetz (former Republican Representative from Utah), and a memorandum sent Elijah J. Cummings (Democratic Representative from Maryland) sent to Democratic members on the committee in response to the report. These timeline events are then corroborated by reporting in the media to paint a clearer picture of the events leading up to the malicious cyber activities in OPM's systems in 2014 and 2015 as well as the events that followed.

The "OPM hack" is in fact a series of multi-stage incidents that resulted in a combined loss of several million data records. The first breach of OPM systems was done by an adversary that managed to exfiltrated sensitive OPM IT architecture information. This first breach,

[65] "Federal Information Security Modernization Act Audit Fiscal Year 2017," 40.
[66] U.S. Congress, House, Committee on Oversight and Government Reform, *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation,* 114th Cong., September 7, 2016, https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf, viii.

detected in early 2014, did not result in the theft of personally identifiable information (PII).[67] The second breach involved three stages, or incidents; as the adversary moved laterally within OPM's network, OPM personnel records, background investigation data, and fingerprint data were exfiltrated across three distinct time periods. Each incident was reported to Congress and the public at large separately. In the end, the data of 4.2 million current and former federal employees, 21.5 million individuals applying for background check investigations with OPM, and 5.6 million fingerprints were stolen.

2.2.1. Burgeoning Intrusions

These breaches were years in the making. Adversaries had access to OPM's network as early as July 2012,[68] as US-CERT (the United States Computer Emergency Readiness Response Team) reported that an OPM server hosted HiKit[69] malware since 2012, meaning that there were already deficiencies in OPM's networks. The first attacker (reported in March 2014 and dubbed "Hacker X1" in the report) gained access to OPM systems in November 2013. In this first known malicious activity, Hacker X1 made off with OPM IT assets, but did not steal any personally identifiable information.[70] The second attacker (identified in April 2015, called "Hacker X2" by the committee) first became active within OPM's networks in December 2013, targeting information hosted by OPM and harvesting credentials from OPM contractors. The

[67] U.S. Congress, House, Committee on Oversight and Government Reform, *Memorandum: Committee Investigation into the OPM Data Breach*, 114th Cong., September 6, 2016, https://democrats-oversight.house.gov/sites/democrats.oversight.house.gov/files/documents/2016-09-06.Democratic%20Memo%20on%20OPM%20Data%20Breach%20Investigation.pdf, 2.

[68] Most timeline items are drawn from a comparison between House Oversight and Government Reform Committee report and the Ranking Member's memo published the day before. See *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation*, 5-13, and *Memorandum: Committee Investigation into the OPM Data Breach.*

[69] The HiKit malware is a rootkit, which provides unauthorized remote access to a computer system or a network interface. More specific details are available at the following link: http://www.novetta.com/wp-content/uploads/2014/11/HiKit.pdf.

[70] Aliya Sternstein and Jack Moore, "Timeline: What We Know About the OPM Breach (UPDATED)," *Nextgov,* June 26, 2015, http://www.nextgov.com/cybersecurity/2015/06/timeline-what-we-know-about-opm-breach/115603/.

same month, hackers breached USIS and KeyPoint Government Solutions, two contractors involved in conducting background check investigations of national security workers.[71]

2.2.2. Command and Control

Once OPM was breached in late 2013 by Hacker X1, the bulk of lateral activity by the attackers within OPM's systems occurred in 2014. OPM also took several counterintelligence measures in response. On March 20, 2014, US-CERT notified OPM of Hacker X1's exfiltration of manuals and IT system architecture information, among other unknown lost data. OPM then implemented a strategy to monitor and gather counterintelligence on the attackers. Five days later, on March 25, OPM CIO Donna Seymour was given a situation report. One week after the initial US-CERT notification, on March 27, OPM also developed what would be known as the "Big Bang," a "plan for full shut down [of systems] if needed" and eventually used as a defensive measure.

April 2014 saw the continuation of operations by both the attackers and OPM in response. OPM continued defensive preparations; on April 11, Donna Seymour was briefed on "tactical mitigation strategies and [a] security remediation plan." On April 21, SRA,[72] an OPM contractor, discovered additional, "specific" malware and notified US-CERT. Several days later, on April 25, the attackers began moving forward with deploying their command and control infrastructure, registering the domain name "opmsecurity.org" to a certain "Steve Rogers" (an alias for "Captain America" in the Marvel movie franchise). This domain would later be used for exfiltration of the data stolen from OPM.

[71] Sternstein and Moore. The USIS intrusion may have occurred as early as April 2013.
[72] SRA was a federal contractor retained by OPM, recently acquired by General Dynamics. For more information, see https://www.csra.com/.

2.2.3. OPM Contractors Breached

By May 2014, the situation grew more complicated, as several OPM contractors who were victim to previous cyberattacks were now losing PII. KeyPoint Government Solutions[73] was breached in a 2014 cyberattack, which resulted in the theft of the PII of roughly 48,000 employees. On May 7, 2014, Hacker X2 "established a foothold into OPM's network" by posing as a KeyPoint employee tasked with performing background checks. Hacker X2 used an OPM credential to remotely access the OPM network and installs PlugX[74] malware to gain backdoor access. Despite OPM deploying counterintelligence measures against Hacker X1, identified by US-CERT back in March 2014, OPM's systems did not successfully detect this intrusion by Hacker X2. Nevertheless, OPM made progress later in the month against Hacker X1. On May 27, OPM noticed that Hacker X1 had loaded keylogging software[75] onto several OPM database administrator workstations and were within earshot to the system holding background investigation data. OPM carried out its "Big Bang" plan to remove Hacker X1 that day by shutting down the compromised those workstations. Furthermore, the Department of Homeland Security "remained with their Mandiant [malware detection and removal] tool for another 30 or 45 days."[76] However, the "Big Bang" event did not flush out Hacker X2, who retained access to the OPM network.

On June 5, malware was successfully installed on a KeyPoint web server. On June 10, OPM CIO Donna Seymour testified before the Senate Homeland Security and Governmental

[73] KeyPoint Government Solutions was a contractor retained by OPM's Federal Investigative Services to perform background investigations to determine suitability for security clearances.
[74] PlugX is another variant of remote access Trojan (RAT) malware. For more information, see here: https://www.lastline.com/labsblog/an-analysis-of-plugx-malware/.
[75] A keylogger may be legal or illegal but used for the express purpose of recording keystrokes and transmitting them back to a central system or server. In OPM's case, the keyloggers installed were clearly used maliciously and illegally for the purposes of cyber theft or cyber espionage.
[76] *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation*, 61.

Affairs' Subcommittee on OPM's *Strategic Information Technology Plan*, released in 2014. In her testimony she does not disclose the March 2014 breach. Additionally, despite being given a clean bill of cyber health by OPM IT security personnel in May 2014, USIS notified OPM in early June about the December 2013 breach.[77] On June 12, OPM and Cylance, an antivirus software firm, reached an agreement that would allow OPM to test two Cylance products--Cylance V and Cylance Protect. Just over a week later, on June 20, Hacker X2 initiated what would be a nearly year-long remote desktop protocol (RDP) session with servers supporting background investigation processes. On June 22, DHS issued a non-public, final incident report for OPM "manuals" breach discovered on March 20, 2014, reporting that "No new systems [were] communicating with known C2 [command and control] servers; no new attacker activity observed."[78] The following day, US-CERT and OPM designate this breach as the "First known adversarial access to OPM's mainframe."

2.2.4. OPM Manuals Breach Draws Public Attention

Over the course of the next two months, in July and August 2014, OPM saw increasing scrutiny from the media, while Hacker X2 exfiltrated background investigation data from OPM. On July 9, OPM acknowledged publicly for the first time that there was a breach of its systems by Chinese hackers back in March 2014, as reported by the *New York Times*.[79] OPM maintained that no PII was lost in the breach but "did not disclose the exfiltration of the manuals." Roughly three weeks later, on July 29, the attackers continued the domain name registration process by registering "opmlearning.org" to "Tony Stark" (the pseudonym of the "Iron Man" character in the Marvel franchise) as another means of command and control. On August 16, the malware

[77] Sternstein and Moore.
[78] *Memorandum: Committee Investigation into the OPM Data Breach*, 6.
[79] Michael S. Schmidt, David E. Sanger, and Nicole Perlroth, "Chinese Hackers Pursue Key Data on U.S. Workers," *The New York Times*, July 9, 2014. https://www.nytimes.com/2014/07/10/world/asia/chinese-hackers-pursue-key-data-on-us-workers.html.

on KeyPoint systems stopped operation. In summary, during these summer months, Hacker X2 successfully stole tens of millions of sensitive background check records from OPM. Also, in August, USIS, an OPM contractor that conducts background checks as part of hiring investigations, was found to have been breached by attackers, thus compromising the personal information of thousands of federal employees.[80]

2.2.5. Attackers "Tap the Mother Lode"[81]

Activities slowed in their pace but not their intensity over the last several months of 2014. In October, the FBI Cyber Division issued a Cyber Flash Alert warning against Chinese government-affiliated cyber actors committing espionage on U.S. commercial and government networks.[82] Hacker X2 remained in the OPM environment and moved to the U.S. Department of Interior (DOI) data center storing OPM personnel records. In November, private-industry cybersecurity companies warned about threats posed to "human resources components of [the] federal government" and releases a report on the Axiom Threat Actor and the Advanced Persistent Threat (APT) group's activities. In December, hacker X2 exfiltrated 4.2 million U.S. federal government employee personnel records from the DOI database holding OPM's personnel records. On December 18, OPM alerted more than 48,000 federal contractors about the exposure of personal information from the KeyPoint breach.[83] Activity quieted the first two months of 2015 and resumed in March 2015. On March 3, attackers registered the domain "wdc-news-post.com", a domain used for command and control and data exfiltration. Nearly a week

[80] *Memorandum: Committee Investigation into the OPM Data Breach*, 4.
[81] Sean Gallagher, "'EPIC fail--how OPM hackers tapped the mother lode of espionage data," *Ars Technica*, June 21, 2015, https://arstechnica.com/information-technology/2015/06/epic-fail-how-opm-hackers-tapped-the-mother-lode-of-espionage-data/.
[82] "FBI Warns U.S. Businesses of China-backed Cyberattacks," *NBC News*, October 15, 2014, https://www.nbcnews.com/tech/security/fbi-warns-u-s-businesses-china-backed-cyberattacks-n226821
[83] Nextgov Staff, "48,000 Federal Employees Potentially Affected by Second Background Check Hack," *Nextgov*, December 18, 2014, http://www.nextgov.com/cybersecurity/2014/12/opm-alerts-feds-second-background-check-breach/101622/.

later, on March 9, traffic to "opmsecurity.org," the domain registered in April 2014 to "Steve Rogers." Investigators found that on March 26, fingerprint data was exfiltrated.

2.2.6. Discovery

OPM conducted significant data collection and analysis of the intruders in its systems in April 2015. On April 15, upon being alerted by SRA, OPM notified US-CERT about suspicious network traffic from OPM's servers to "opmsecurity.org." This sequence of events corroborates Ranking Member Cummings' memo detailing that "OPM discovered the breach on April 15 or 16, 2015," not a third-party entity.[84]

The next day, April 16, two significant events occurred. First, Brendan Saulsbury, an OPM contract engineer who detected an unknown SSL (Secure Socket Layer) certificate as part of his contract work within the agency's Security Operations Center, reportedly detected malicious activity from malware disguised as an antivirus software file "beaconing out to a command and control server from, at the time, two different servers."[85] Second, OPM first contacted Cylance regarding the Cylance V product it had purchased on September 4, 2014. While the House Committee report notes that Cylance V "is not intended to be an enterprise-wide prevention tool,"[86] it nonetheless was crucial in detecting network anomalies and the existence of malware on OPM's systems.

The following day, April 17, OPM deployed CylanceProtect, an enterprise-wide protection tool, on its systems and called in Cylance onsite for incident response. Over the course of the next two days, April 18 to April 19, CylanceProtect is deployed to over 2,000 devices and found malicious activities within OPM systems. CyTech Services, a network forensics provider, was hired by OPM on April 21 to provide a demonstration of its CyTech

[84] *Memorandum: Committee Investigation into the OPM Data Breach*, 7.
[85] Ibid., 8.
[86] *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation*, 10.

Forensics and Incident Response (CyFIR) tool the following day. CyTech would stay onsite until May 1. The distinction between Cylance and CyTech must be made here: despite CyTech's claims that it had first discovered malware on OPM's systems (and therefore the breach), OPM's Director of Security Operations, Jeff Wagner, spoke on the record about contacting then-OPM CIO Donna Seymour on April 17, 2015--five days before CyTech's product demonstration--about the Cylance product assisting with forensics and finding malware on OPM's network.[87]

On April 22, Donna Seymour testified before the House Oversight and Government Reform Committee about the "manuals" breach from March 2014. That same day, the OPM Office of the Inspector General (OIG) learns about the breach for the first time. The next day, April 23, OPM determined that the exfiltration of personnel records constituted a "major incident," triggering a requirement to notify Congress. On the system protection from, OPM ordered a global quarantine of the malware found by CylanceProtect. On April 26, Cylance identified the June 2014 RDP session established by Hacker X2 back in June 2014. On April 30, a week after triggering the Congressional notification requirement, OPM notified Congress.

In May and June 2015, OPM continued to notify Congress of the different stages of the data breach and received considerable attention in the press. On May 8, US-CERT established "with a high degree of certainty that personnel records data/PII had been stolen." On May 20, OPM determined that the exfiltration of background investigation data also constituted another "major incident," triggering another requirement to notify congress; OPM notified Congress a week later, on May 27. At this time, OPM also notified the OIG about potential background investigation information compromise. On June 4, 2015, OPM briefed the media and issued a press statement on the loss of 4.2 million former and current federal employee personnel

[87] *Memorandum: Committee Investigation into the OPM Data Breach*, 9.

records. On June 8, a month after US-CERT evaluated the loss of personnel data records, it again established "with a high degree of certainty that background investigation data/PII [had] been exfiltrated and stolen." By this time, the breach had reached the highest ranks of leadership at OPM. On June 16, 2015, OPM Director Katherine Archuleta publicly acknowledged that background investigation data may have been compromised in a separate breach. OPM also estimated that 1.1 million fingerprint records had been lost that same summer. Archuleta blamed OPM's lax security practices and procedures, including a lack of basic encryption, on antiquated systems.

2.2.7. Immediate Fallout

On June 23, Director Archuleta testified at a Congressional hearing that hackers used comprised KeyPoint user credentials to access OPM's network.[88] On June 24, 2015, Donna Seymour again testified before the House Committee to minimize the impact of the 2014 "manuals" breach. Late that month, on June 29, the American Federation of Government Employees (AFGE) filed a class action lawsuit against OPM for the data breaches (although these suits were dismissed in September 2017). Mitigation and other defensive procedures continued all the same, with CylanceProtect detecting and blocking nearly 2,000 pieces of malware across over 10,250 devices. The same month, OPM released a document titled, "Actions to Strengthen Cybersecurity and Protect Critical IT Systems" to discuss actions taken by OPM about security breaches, actions to mitigate security breaches currently underway, and future proposed actions in response to the incident. OPM provided a list of 23 action items that the agency took under then-Director Archuleta's leadership, and a list of 15 new actions to

[88] Sternstein and Moore.

"bolster and modernize IT systems."[89] However, the plan may have proved too little, too late, as fallout from the incident continued into the summer and the backlash grew more tumultuous.

In a House Oversight Committee hearing about the OPM data breach on June 24, 2015, Chairman Chaffetz and 17 other Republican members of the committee requested the removal of then-OPM CIO Donna Seymore and then-OPM Director Katherine Archuleta.[90] On July 9, OPM confirmed 21.5 million background investigation records were compromised. The next day, July 10, Katherine Archuleta resigned as OPM director. The same day, Beth Cobert was appointed as Acting Director of OPM, thus beginning a nearly three-year period during which OPM was without the leadership of a permanent Director. Shortly after the breaches, OPM awarded a $20 million-plus contract for identity protection from Austin, Texas-based firm CSID. Upon acknowledging that the OPM breach included more than 5.6 million sets of fingerprints in September 2015 (five times the original 1.1 million amount),[91] OPM awarded a $133 million contract to the Portland, Oregon-based private firm ID Experts to provide similar identity protection services, although security experts have doubted the extent to which such services would adequately protect the future privacy of the affected data breach victims.[92]

2.2.8. Later Developments and OPM Today

On July 21, the House Oversight and Government Reform Committee began its investigation of the OPM incidents, requesting documents from the agency. On August 20, OPM returned the CyFIR tool to CyTech. On September 23, 2015, OPM updated its estimate of

[89] U.S. Office of Personnel Management, "Actions to Strengthen Cybersecurity and Protect Critical IT Systems." June 2015. https://www.opm.gov/cybersecurity/cybersecurity-incidents/opm-cybersecurity-action-report.pdf.
[90] *Memorandum: Committee Investigation into the OPM Data Breach*, 17.
[91] Andrea Peterson, "OPM says 5.6 million fingerprints stolen in cyberattack, five times as many as previously thought," *The Washington Post*, https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/?utm_term=.7cdc1f94edd5.
[92] Brian Krebs, "OPM (Mis)Spends $133M on Credit Monitoring," *Krebs on Security*, September 2, 2015, https://krebsonsecurity.com/2015/09/opm-misspends-133m-on-credit-monitoring/.

fingerprint records lost to 5.6 million, from an original estimate of 1.1 million. On February 22, 2016, OPM CIO Donna Seymour resigned. On September 6, the Ranking Member of the House Committee on Oversight and Government Reform, Elijah Cummings of Maryland, released a memo sent to Democratic members of the Committee in anticipation of the release of the Majority Staff report, under the leadership of Chairman Jason Chaffetz of Utah, on the OPM data breaches. The next day, the Republic leadership in the Committee released the report.

When the Trump administration began on January 20, 2017, Acting Directorship of the agency transitioned from Beth Cobert to Kathleen McGettigan, an OPM veteran. Slightly over a year later, on March 8, 2018, the Senate voted to confirm the nomination of Jeff T. H. Pon as permanent OPM director after a lengthy confirmation process that included a brief political struggle between the Senate Homeland Security and Governmental Affairs Committee and OPM over document requests and the separate, failed nomination of an OPM veteran as a candidate who withdrew from federal employee backlash and background check concerns.[93] On March 12, 2018, Jeff Pon began his appointment as the 11th Director of the U.S. Office of Personnel Management, starting alongside the new Deputy Director, Michael Rigas.[94]

In September 2017, U.S. District Judge Amy Jackson of the U.S. District Court for D.C. dismissed two separate lawsuits filed by the National Treasury Employees Union and the American Federation of Government Employees, citing the lack of the plaintiffs' standing[95] and the "difficulty of legally proving harm as the result of having personally identifiable

[93] Erich Wagner, "OPM Gets a Permanent Director After Nearly 3 Years of Acting Leaders," *Government Executive*, March 8, 2018, https://www.govexec.com/management/2018/03/senate-confirms-opm-director/146499/.
[94] U.S. Office of Personnel Management, Office of Communications, "OPM welcomes Dr. Jeff T.H. Pon as 11th director of the agency," *OPM.gov*, March 12, 2018, https://www.opm.gov/news/releases/2018/03/opm-welcomes-dr-jeff-t-h-pon-as-11th-director-of-the-agency/.
[95] Morgan Chalfant, "Court dismisses lawsuits over OPM data breach," *The Hill*, September 19, 2017, http://thehill.com/policy/cybersecurity/351395-court-dismisses-lawsuits-over-opm-data-breach.

information (PII) stolen."[96] Today, OPM still offers online resources for individuals who were impacted by both the background check and personnel records cyber incidents. Four services are provided: identity monitoring, credit monitoring, identity restoration services, and identity theft insurance.[97]

2.3 Notable Actors

Better understanding both the defensive and offensive actors during the OPM data breach incidents allows builds crucial context in analyzing the capabilities and preparedness of either side as they relate to each other. Three major sets of players (two from the defensive perspective, and one from the offensive perspective) are relevant to the discussion of the OPM case study: 1) the U.S. federal government, including OPM and other relevant agencies responsible for detecting and responding to the breaches; 2) federal contractors, whose relationships with the U.S. federal government was targeted and exploited to break into OPM; and 3) Chinese-government backed Advanced Persistent Threats (APTs), which many security analysts would attribute to be behind the OPM breach.

2.3.1. Defensive: U.S. Federal Government Agencies

Most of the actors within the U.S. federal government during this time were members of OPM leadership. In addition, OPM partnered with the U.S. Department of Homeland Security's U.S. Computer Emergency Readiness Team (US-CERT) to investigate and mitigate the data breaches. Additionally, OPM received law enforcement assistance from the Federal Bureau of Investigation (FBI) in the search for the authors of the command and control malware installed onto their servers. Two primary offices within OPM set the policy direction for information

[96] David Thornton, "Judge dismisses OPM data breach lawsuits, union appeals," *Federal News Radio*, September 21, 2017, https://federalnewsradio.com/opm-cyber-breach/2017/09/judge-dismisses-opm-cyber-breach-lawsuits-union-appeals/.
[97] U.S. Office of Personnel Management, "Cybersecurity Resource Center," *OPM.gov*, https://www.opm.gov/cybersecurity/.

security and cybersecurity preparedness. The Office of the Chief Information Officer reports directly to the Office of the Director. The OPM Director presiding over the data breaches was Katherine Archuleta, who was appointed by President Obama on May 23, 2013, sworn in on November 4, 2013,[98] and ultimately resigned on July 10, 2015 from bipartisan fallout over the OPM breaches. Critics argued that Archuleta lacked a particular expertise in cybersecurity for decision-making during the breach.[99]

Upon Archuleta's resignation, Beth Cobert took over as Acting Director of OPM in July 2015. Reporting directly to both Archuleta and Cobert was the OPM Chief Information Officer, Donna K. Seymour, who served in the role from December 2013 until February 2016. During her tenure as CIO, Seymour "turned an 'array of aging systems' into a more 'modern, secure environment… to better protect [OPM's] existing legacy systems.'"[100] Despite mounting pressure for her firing in the months leading up to her resignation, Seymour was a federal service veteran who led an aggressive effort to find the intruders in OPM's network.[101]

US-CERT was created in September 2003 to "protect the Nation's Internet infrastructure by coordinating defense against and response to cyberattacks."[102] US-CERT works with federal agencies, the private sector, the research community, state and local governments, and international entities to provide detection, data collection, analysis, containment, and decontamination measures in response to cyber incidents. During the OPM breaches, the

---

[98] An archive of Katherine Archuleta's staff biography is available at the following URL: https://www.opm.gov/about-us/our-people-organization/senior-staff-bios/katherine-archuleta/.
[99] Julie Hirschfeld Davis, "Katherine Archuleta, Director of Personnel Agency, Resigns," *The New York Times*, July 10, 2015, https://www.nytimes.com/2015/07/11/us/katherine-archuleta-director-of-office-of-personnel-management-resigns.html.
[100] Angus Loten, "OPM CIO Resigns, but Blame for Data Breach Lingers," *The Wall Street Journal*, February 23, 2016, https://blogs.wsj.com/cio/2016/02/23/opm-cio-resigns-but-blame-for-data-breach-lingers/.
[101] Aaron Boyd, "OPM CIO Seymour resigns days before Oversight hearing," *Federal Times,* February 22, 2016, https://www.federaltimes.com/it-networks/2016/02/22/opm-cio-seymour-resigns-days-before-oversight-hearing/.
[102] U.S. Department of Homeland Security, United States Computer Emergency Readiness Team, "Information Sheet: US-CERT," *US-CERT*, https://www.us-cert.gov/sites/default/files/publications/infosheet_US-CERT_v2.pdf.

agency not only reported information about the breaches to US-CERT, but also worked with US-CERT to develop the "Big Bang" counterintelligence plan in March 2014 and detect and remove the intruders stealing OPM data in the early months of 2015. In 2017, the U.S. Department of Homeland Security streamlined the organizational structure National Cybersecurity and Communications, integrating US-CERT into a single, broader National Cybersecurity and Communications Integration Center (NCCIC) structure, which seeks to "reduce the risk of systemic cybersecurity and communications challenges in [its] role as the Nation's flagship cyber defense, incident response, and operational integration center."

Law enforcement agencies also play a role in cyber incident response. On June 4, 2015, OPM announced that it was partnering with the FBI in addition to DHS to investigate the impact of the incident on federal personnel; the FBI confirmed its cooperation with OPM the same day.[103] The next day, the FBI issued a Flash Alert detailing the technical workings of Sakula, a form of malware known as a remote access trojan (RATs) that was used by malicious groups to compromise and steal PII.[104] This revelation was done much to the delight of the cybersecurity research community, which speculated that those were the same RATs used in the OPM data breaches.[105, 106] The FBI's cooperation yielded promising results in due time. In August, 2017, the FBI arrested a Chinese national related to the creation of the Sakula malware.[107]

---

[103] U.S. Department of Justice, Federal Bureau of Investigation, "FBI Investigating OPM Cyber Intrusion," *FBI.gov*, June 4, 2015, https://www.fbi.gov/news/stories/fbi-investigating-opm-cyber-intrusion.
[104] U.S. Department of Justice, Federal Bureau of Investigation, Cyber Division, "FBI FLASH: Alert Number A-000061-MW." June 5, 2015. https://info.publicintelligence.net/FBI-HackToolsOPM.pdf.
[105] FCW Staff, "Revealing the RATs and scoring the agencies," *FCW*, June 29, 2015, https://fcw.com/articles/2015/06/29/news-in-brief-june-29.aspx?s=fcwdaily_300615.
[106] Cory Bennett, "FBI: Chinese malware possibly behind OPM hack," The Hill, July 2, 2015, http://thehill.com/policy/cybersecurity/246754-fbi-warns-of-chinese-malware-possibly-behind-opm-hack.
[107] Evan Perez, "FBI arrests Chinese national connected to malware used in OPM data breach," *CNN*, August 24, 2017, https://www.cnn.com/2017/08/24/politics/fbi-arrests-chinese-national-in-opm-data-breach/index.html.

2.3.2. Defensive: Affected Federal Contractors in Background Investigations and Healthcare

Several OPM contractors that provided investigative background check and healthcare services for OPM were targeted around the time of the OPM breaches. These contractors include: U.S. Investigations Services, LLC (USIS); KeyPoint Government Solutions; Anthem; and Premera. According to the House Oversight committee report, USIS was the largest background investigation contractor and detected a June 2014 cybersecurity breach carried out by a state-sponsored actor (an Advanced Persistent Threat, or APT) that affected the PII of over 31,000 background check investigations for the Department of Homeland Security. USIS had mitigated the breach in July 2014 and publicly acknowledged the breach in August 2014. As it appeared that the APT was going after background investigation data, the U.S. Computer Emergency Readiness Team (US-CERT) approached KeyPoint to assess the security of the contractor. In December 2014, KeyPoint had also been breached, affecting the PII of over 48,000 federal employees. In June 2015, the CEO of KeyPoint confirmed that the user credentials of an employee at the company were compromised in order to gain access to OPM.[108]

Anthem and Premera were two healthcare-related OPM contractors that were breached during the course of events in the OPM incident. In February 2015, Anthem, which provides healthcare coverage for 1.3 million federal employees, announced a data breach of 80 million healthcare records of current and former customers and employees. The next month, in March 2015, Premera, with an OPM contract covering 130,000 federal employees, announced a data breach exposing medical data and financial information of 11 million customers. Therefore, as part of a multi-stage intrusion, a total of tens of millions of contractor records related to

[108] *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation*, 31-32.

background check investigations and healthcare information were harvested by adversaries in order to gain access into OPM and exfiltrate data.

2.3.3. Offensive: Chinese-Government Backed Advanced Persistent Threats (APTs)

After a network or computer system intrusion has occurred and is detected, attribution is important for both intelligence gathering purposes and reassurance to the public. For many nation-state governments, attribution is a tricky balancing act. On one side, in the face of a major data breach or a cyber incident, there is a prerogative to be transparent as possible about the details of such an incident to reassure the public. In a cyber status quo with few norms and written rules of engagement, attribution also plays a critical role in "naming and shaming" as part of a nation's foreign policy toolkit. On the other hand, revealing too much information can be a double-edged sword, as many technical details used to justify an attribution to another actor may also reveal the sources and methods used by the defending nation-state to detect and respond to cyber incidents.

Against this complicated and nuanced technical, diplomatic, and intelligence backdrop, the U.S. government was initially mum about publicly attributing the OPM breach to any specific nation-state actor. In late July, 2015, U.S. officials were reluctant to publicly blame China for the OPM intrusion "out of reluctance to reveal the evidence that American investigators have assembled"[109] ahead of a state visit by Chinese President Xi Jinping to the United States. In December 2015, the Chinese government claimed that it had arrested the hackers responsible for the OPM breaches earlier in the year, characterizing the activity as a criminal matter rather than state-sponsored action.[110] Nevertheless, leadership in the intelligence community, such as

[109] Ellen Nakashima, "U.S. decides against publicly blaming China for data hack," *The Washington Post*, July 21, 2015, 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?utm_term=.a5aea01795eb.
[110] Ellen Nakashima, "Chinese government has arrested hackers it says breached OPM database," *The Washington Post*, December 2, 2015, https://www.washingtonpost.com/world/national-security/chinese-government-has-

former Director of National Intelligence James Clapper, noted that the OPM breach was an example of sophisticated intelligence work outside the scope of normal industrial espionage.[111]

The OPM data breaches were eventually linked to a Chinese-government backed advanced persistent threat (APT) by both indirect government attribution and publicly available intelligence analyzed by the cybersecurity research community. APTs are "well-financed, often state-sponsored team[s] of hackers."[112] APTs such as the Chinese People's Liberation Army Unit #61398 are extensions of the Chinese military and have been documented as having conducted cyber espionage since at least 2006.[113] Although Unit #61398 may not have been the precise actor that targeted the OPM data, the kinds of activities it conducts and the support it receives from the Chinese government are indicative of the potential havoc an APT can wreak upon its targets.

Outside of government, security researchers found strong ties to Chinese-based actors from the command and control infrastructure detected in the breach, linking the malicious activity to not only OPM but the Anthem, Premera, and other healthcare-based organization breaches. Additionally, the researchers were able to tie the Sakula-based RAT malware to the registration of domain names used for the malicious command and control infrastructure used in the exfiltration of data. In September 2017, the FBI arrested the author of the malware Yu Pingan, also known as "GoldSun," furthering the China-OPM breach link.

---

arrested-hackers-suspected-of-breaching-opm-database/2015/12/02/0295b918-990c-11e5-8917-653b65c809eb_story.html?utm_term=.23171c02d1fc.

[111] Elias Groll, "Clapper: 'We Don't Know Exactly What Was Taken in the OPM Breach,'" *Foreign Policy*, September 24, 2015, http://foreignpolicy.com/2015/09/24/clapper-we-dont-know-exactly-what-was-taken-in-the-opm-breach/

[112] Koerner.

[113] Mandiant Intelligence Center,"APT1: Exposing One of China's Cyber Espionage Units," *Mandiant*, February 19, 2013, https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

2.3.4. Relationship between Actors

The relationship between the actors in the OPM breaches may be contextualized by the framework offered in Buchanan's cybersecurity dilemma. From the defenders' (U.S. government and federal contractors) perspective, a baseline network defense model involves preparation, detection, data collection, analysis, containment, and decontamination. While OPM and its federal contractors were arguably ill-prepared for such a sophisticated, multi-stage intrusion from a foreign intruder, detection was the most difficult step, as it took OPM several months in the timeline of events before it noticed that there was suspicious cyber activity within its network. Once OPM had ascertained that a stolen contractor credential had been used for the unauthorized access of data, its later investigative efforts alongside US-CERT and the FBI greatly accelerated the data collection, analysis, containment, and decontamination steps.

From the offensive perspective (Chinese government-backed APTs), the multi-step intrusion model--target acquisition, development, authorization, entry, command and control, pivoting, payload activation, and confirmation--may be applied in better understanding some of the details of the OPM breach. It seems clear now that target acquisition was primarily the sensitive PII of U.S. federal government employees and contractors, most likely for counterintelligence purposes. The development and authorization stages are hazy as they are beyond the scope of this thesis. However, from information gleaned about the OPM breaches, the intruders' method of entry was clear (stealing contractor credentials before entering OPM's systems); their command and control infrastructure has been revealed (the Sakula malware used to communicate); and their pivoting, payload activation, and confirmation details contained in publicly available government reports. The OPM data breaches are an example of the majority of offensive actions taken first, before defensive measures could be used to stem the impact of the incidents.

Part Three: Diagnostics of the OPM Failure

With a timeline of the OPM breaches and a wider fact base established, this chapter (1) discusses the technical elements behind the OPM data breaches; (2) examines the policy, personnel, and management elements leading to the OPM data breaches; (3) analyzes OPM's FISMA compliance audit data from 2007 to 2017 to provide insight on the agency's historical cybersecurity preparedness and posture; and (4) evaluates the various technical, management, and compliance factors in OPM's failure to secure its information assets.

3.1. Overview of Technical Elements behind the OPM Data Breaches

Over the course of many months, adversaries exploited a combination of vulnerabilities to conduct a sophisticated, multi-stage cyber espionage operation[114] on the U.S. Office of Personnel management. The first step of the espionage operation involved systematically penetrating the networks of various OPM investigations and healthcare contractors in an effort to obtain login credentials.[115] Next, the intruders moved laterally within the OPM network and deployed a malware payload for command and control operations. Then, data from OPM were systematically exfiltrated via the command and control infrastructure. While OPM worked to flush out one set of attackers from a previous cyber incident that did not result in the loss of PII, the agency did not detect a second intruder's presence, which would later result in the loss of millions of records. An OPM security contractor detected network traffic anomalies and strange files indicative of a malware attack, triggering a larger response to the second attacker's presence that would eventually break the news of the breach.

[114] *Memorandum: Committee Investigation into the OPM Data Breach.*
[115] Ibid., 5

3.1.1. The Axiom Group and HiKit Malware in the "Manuals" Breach

In the investigation of the OPM "manuals" breach, US-CERT had found Hikit malware on several OPM systems as early as 2012;[116] the House Oversight and Government Reform Committee concluded that the OPM data breach discovered in March 2014 originated from the Axiom Group,[117] a state-sponsored threat actor, based on the presence of the Hikit malware and other tactics, techniques, and procedures associated with the group that have been publicly reported in the past.[118]

Two variants of the Hikit malware, known as Hikit A and Hikit B, were used in the OPM "manuals" breach discovered in March 2014; there is no indication that OPM understood how the attackers initially gained entry into OPM's system.[119] Hikit installs itself as a network adapter between the physical network interface and network protocol drivers, so that it can monitor incoming traffic, intercept command and control data from outside infrastructure, and then parse the commands.[120] Such operations allow the malware to "phone home" for commands as well as transmit stolen information assets. While no personally identifiable information was taken during this breach, the intruders did have access to the OPM server containing background investigation materials. The information taken about OPM's systems that may have given future adversaries details about the architecture of OPM's environment that would later be useful in stealing sensitive personnel data and other PII.

---

[116] *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation*, 5.
[117] Novetta and the Cyber Security Coalition, "Operation SMN: Axiom Threat Actor Group Report 公理队," *Novetta*, October 27, 2014, http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf.
[118] *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation*, 5.
[119] Ibid., 13-14.
[120] Christopher Glyer and Ryan Kazanciyan, "The 'Hikit Rootkit: Advanced and Persistent Attack Techniques (Part 2)," *FireEye*, August 22, 2012, https://www.fireeye.com/blog/threat-research/2012/08/hikit-rootkit-advanced-persistent-attack-techniques-part-2.html.

3.1.2. Contractor Access and Permissions in the Second Data Breach

The federal government works with many contractors to conduct certain functions within the bureaucracy. OPM in particular contracted work with third-party background check investigation providers and healthcare providers as part of its human resources and vetting mission. Specifically, in a December, 2014 breach, KeyPoint Government Solutions, an OPM investigations contractor had been breached, resulting in the loss of PII for over 48,000 of its employees and the theft of legitimate login credentials that would enable a user to gain access to OPM's systems. According to the House report on the OPM breach, the exact process by which OPM attackers were able to steal a valid credential from KeyPoint remains unclear. Nevertheless, attackers then exploited this legitimate login credential as a vector of infection to then tunnel into the OPM network via a virtual private network (VPN) and install a malware payload, providing command and control access from afar.[121]

Using the stolen credentials from KeyPoint and the VPN session, attackers first gained access to an SQL database server and opened a remote desktop connection (RDP) to deploy the malware payload. Information security at OPM explained that the SQL server served as a firewalled "back end storage" for various OPM application, separate from the normal OPM network. Next, the attackers dropped a malware payload of the PlugX malware on fewer than 10 OPM machines, but these machines included what is known as a "jumpbox," which is the administrative server used to log into all other servers in OPM's network.[122] The attackers then moved laterally from the SQL server to other areas of the OPM network to then exfiltrate sensitive personnel, background check, and fingerprint data.[123]

---

[121] David Kennel, "OPM vs. APT: How Proper Implementation of Key Controls Could Have Prevented a Disaster," *SANS Institute*, March 10, 2016, https://www.sans.org/reading-room/whitepapers/breaches/opm-vs-apt-proper-implementation-key-controls-prevented-disaster-36852, 8.
[122] Koerner.
[123] *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation*, 87-89.

3.1.3. DeepPanda's Command and Control: PlugX and Sakula Family of Malware

Researchers have linked the activities involved in the data breaches discovered in April 2015 to the group "DeepPanda," another suspected state-sponsored threat-actor group.[124] The command and control (C2) infrastructure used by the intruders in the OPM breach shared many of the same characteristics of the C2 infrastructure used in the OPM contractor breaches. This infrastructure consists of a series of thematically similar registered domain names traced back to registrants in China and two forms of malware that communicated with the Internet Protocol (IP) addresses associated with those domain names. The 2016 House Oversight and Government Reform Committee notes that PlugX[125] malware was used by the attackers from May into June 2014, which enabled the attackers to evade the May 27, 2014, "Big Bang" event that flushed out the first set of intruders from OPM's systems. US-CERT had evidence from as early as July, 2014, that the attackers began to exfiltrate background investigation data using encrypted Roshal Archives (compressed files with the .RAR extension). The exfiltration of background check data continued until August, 2014. Several months later, on March 26, 2015, the attackers began exfiltrating fingerprint data from OPM's network.

PlugX is a "remote-access tool commonly deployed by Chinese-speaking hacking units."[126] It contains modular plugins and allows the attacker 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."[127] US-CERT found evidence that the PlugX malware communicated with "opmsecurity.org," another part of the C2 infrastructure used for data exfiltration. In fact, the House investigation revealed that the PlugX

[124] *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation*, 18.
[125] "PlugX," *NJ Cybersecurity & Communications Integration Cell*, April 12, 2017, https://www.cyber.nj.gov/threat-profiles/trojan-variants/plugx.
[126] Koerner.
[127] *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation*, 86.

was deployed again into OPM's systems on October 10, 2014, and then once more on January 15, 2015, suggesting that "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."[128] All of these actions point to the work of a sophisticated cyber actor that knows is technically competent and well-resourced to continue such operations. According to security researchers analyzing publicly available information, the links to the command and control infrastructure were also closely tied to the modus operandi of previous attacks on OPM contracts, including Anthem and Premera. In all of these breaches, researchers have high confidence that intruders also used Sakula malware to facilitate the exfiltration of files. The Sakula malware variant had a file signature to unique infrastructure specifically designed for persistence.

The Sakula malware is a remote access trojan (RAT) for the Microsoft Windows platform that first surfaced in 2012 and used until 2015. Once infected, Sakula remains persistent by setting a Microsoft Windows registry key and installing itself as various new services. To avoid detection by a user on an infected system, Sakula uses Windows DLL (a software library) sideloading and masquerades itself as an antivirus software (Kaspersky or McAfee--a McAfee DLL was found by Brendon Saulsbury, the contractor who first detected suspicious communications activities from OPM's network). Sakula also uses single-byte XOR, a binary logical operator, to disguise many of its files from the infected host operating system. Once installed, Sakula can use the Windows command line interface, download files remotely, delete temporary files, and perform cleanup. Sakula contains code to bypass Windows User Account Control, which allows it to run any program on an infected computer. Sakula communicates

[128] *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation*, 86.

with C2 infrastructure using HTTP and encodes outgoing C2 traffic with a custom cryptographic protocol (single-byte XOR) keys.

The campaign that used the Sakula family of malware had many similarities to another campaign that targeted a Virginia-based defense contractor, VAE, Inc. There were also strong ties between the OPM incident and attacks with similar domain name registrations. These registrations included Marvel "Avengers" franchise themed first and last names and temporary email accounts of random alphabetic characters at the gmx.com domain name. Finally, independent security researchers indicated with a high degree of confidence that the kinds of breaches that USIS had experienced in 2013, as well as 2015 breaches of federal healthcare providers such as Anthem, Premera, Empire, and Carefirst, shared similar characteristics as the breach of OPM in July 2014. They were able to link the malware to an APT from China known as "Deep Panda," which targeted similar PII data, such as names, employment history, and Social Security numbers that were also targeted in the healthcare provider breaches. Such evidence provides a stronger sense of correlation than mere coincidence.[129]

3.2: Policy, Personnel, and Management Elements Leading to the Incidents

Three policy, personnel, and management elements were major contributions to the OPM data breach. First, a gap in technology leadership in OPM caused it to fail to properly heed previously warnings about its IT security practices, despite years of internal warnings and a pattern of similar malicious activity that affected its contractors. Second, OPM's poor implementation of certain security practices (using available technical resources) made it more likely to be penetrated. Finally, issues in data access and management policies, particularly with contractors, made OPM more susceptible to a breach.

[129] "OPM Breach Analysis: Update," *ThreatConnect*, June 9, 2015, https://www.threatconnect.com/blog/opm-breach-analysis-update/.

3.2.1. Lack of IT Leadership and Missed Warnings

While a shortage of specific cybersecurity expertise is by no means an indictment against the success of agency leadership, the fact pattern revealed in this paper shows that then-OPM Director Katherine Archuleta, several of her predecessors, and the Office of the Chief Information Officer (OIG) failed to prioritize the technology safety of OPM, amounting to a lack of IT leadership. Specifically, during the first and second breaches of OPM's network in 2014 and 2015, the OCIO failed to give timely notification to the OPM Office of the Inspector General (OIG) of the 2014 and 2015 data breaches or whether the data were compromised; the OCIO failed to notify the OIG of major IT investments to develop a new IT infrastructure; and OPM did not disclose the September, 2014, breach of a major contractor, KeyPoint, to the OIG. Indeed, watchdog groups such as the OPM OIG may be stringent in evaluating agency compliance with certain federal standards, but the end result of such audits are to maintain high-quality government services. At the very least, the three missteps noted above indicate reluctance for OPM leadership at the time to coordinate the beginnings of an effective response.

Furthermore, Office of Personnel management has "historically maintained a fragmented IT infrastructure, and still lacks a full, accurate inventory of all its major IT systems." According to the 2016 House Oversight and Government Reform committee report, OPM "failed to sufficiently respond to growing threats of sophisticated cyber attackers;" "failed to prioritize resources for cybersecurity," and largely ignored a 2005 warning from its Inspector General of the strategic and intelligence value of the sensitive data OPM holds on its employees and their family members.[130] OPM's management also missed warnings from the U.S. intelligence community dating to roughly 2010, when they expressed concerns about the

[130] *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation*, 24.

privacy, security, and data ownership impacts merging intelligence agency employees databases with OPM personnel data, citing the dangers exposing the PII of covert operatives in the field should hackers gain access to OPM systems.[131]

The fact pattern gleaned from contemporary news articles from the time demonstrates that malicious actors were already targeting the data of U.S. workers, whether they be federal employees or federal contractors. Public news outlets noted as early as July 2014 that the March 2014 OPM "manuals" breach indicated that foreign actors were indeed interested in the PII of federal workers.[132] Internally, OPM did respond by formulating counterintelligence activities and developing the "Big Bang" plans, but the timeline indicates that perhaps OPM leadership were overconfident in the "Big Bang" event's ability to flush out attackers and missed the possibility that another malicious actor could have been inside OPM's network. Despite the pattern of data breaches that overcame key OPM contractors noted above, including USIS, KeyPoint, Anthem, and Premera, it at least seems publicly that OPM leadership missed the connection between the contractors and the agency itself.[133] Coupled with the warnings from the Inspector General's FISMA audits, OPM's leadership could have been more responsive to events at the time in relation to its recorded, historical weaknesses.

3.2.2. Inadequate Implementation of Multifactor Authentication

A specific vulnerability (or perhaps, feature) within OPM's network that hackers exploited was that any OPM employee or contractor could login with only a username and password. Using a stolen KeyPoint credential, attackers were able to login to OPM's systems.

---

[131] Shane Harris, "Spies Warned Feds About OPM Mega-Hack Danger," *The Daily Beast*, June 30, 2015, https://www.thedailybeast.com/spies-warned-feds-about-opm-mega-hack-danger.
[132] Michael S. Schmidt, David E. Sanger, and Nicole Perlroth,"Chinese Hackers Pursue Key Data on U.S. Workers," *The New York Times*, July 9, 2014, https://www.nytimes.com/2014/07/10/world/asia/chinese-hackers-pursue-key-data-on-us-workers.html.
[133] Koerner.

While this kind of single-factor, knowledge-based authentication is generally secure, multi-factor authentication that has involves another form of user and identity verification enhances access controls.[134] Multi-factor authentication requires a secondary or other form of authentication in addition to a username and password. Multi-factor authentication is a useful protection in the case a credential set with a username and a password is stolen or otherwise compromised, as the combination of a username and password alone would not be sufficient to access a system or gain entrance into a network. For the federal government, this multifactor authentication device was a PIV (Personal Identity Verification) card, an identification card containing a chip to be slotted into a reader when logging into an OPM system. OPM had worked to strengthen access controls with PIV multi-factor authentication as early as September, 2009.[135] Unfortunately, OPM did not implement multi-factor authentication until January, 2015--over four years later--when attackers already had access to OPM's network and deployed malware to exfiltrate the data.

3.2.3. Data Management Policy Issues

The records stolen in the breach resided in three different locations. First, background investigation was stored in the PIPS (Personnel Investigations Processing System) database. Second, fingerprint records were stored in OPM's FTS (Fingerprint Transaction System). Third, OPM's personnel information were not actually stored within OPM's network but was actually housed within the Department of the Interior (DOI). PIPS and FTS, the two systems storing data within OPM's network, relied on proper authorizations from the overall OPM network infrastructure to operate. Over the course of the House Oversight and Government Reform

[134] U.S. Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory, Applied Cybersecurity Division, Trusted Identities Group, "Back to basics: Multi-factor authentication (MFA)," https://www.nist.gov/itl/tig/back-basics-multi-factor-authentication.
[135] *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation*, 39.

Committee investigation, it was found that OPM's LAN/WAN (Local Area Network/Wide Area Network) and ESI (Enterprise Server Infrastructure) environments, spread across OPM headquarters in Washington, D.C.; a data center in Boyers, Pennsylvania; and a backup data center in Macon, Georgia, were all running on expired Authorities to Operate.[136]

More problematic was the fact that personnel records were hosted by the Department of the Interior, as hosting data in a separate facility exposes the second facility to much greater cyber risk. A remote desktop session enabled the hackers to tunnel into the DOI's systems and to where the OPM personnel data was held. From a July 15, 2015 hearing, "Cybersecurity at the U.S. Department of Interior," DOI leadership testified that "the adversary had access to [DOI's] data center…[but] there was no evidenced based on the investigation that was led by DHS, US-CERT, and the FBI… that the adversary had compromised any other data aside from the OPM data."[137] Nevertheless, such information storage practices unnecessarily jeopardized DOI, which hosted the data. If the attackers had been more aggressive, or had known about the DOI's information system architecture, the scope of the breach could have been much greater.

Furthermore, OPM took on increased risk from malicious cyber activities by not fully encrypting its IT systems. A lack of encryption was not for want of technical resources, but rather a lack of In a June 16, 2015 House Oversight and Government Reform Committee hearing, then-OPM Director Archuleta indicated that OPM had procured the tools for the encryption of its databases but that the agency encountered difficult in encrypting its legacy IT systems because the older hardware did not support such encryption schemes.[138] Outside

---

[136] *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation*, 48-49.
[137] U.S. Congress, House, Committee on Oversight and Government Reform, Subcommittee on Information Technology, *Cybersecurity: The Department of the Interior*, 114th Cong., 1st sess., July 15, 2015. https://oversight.house.gov/wp-content/uploads/2016/04/7-15-15-Cybersecurity-The-Department-of-the-Interior.pdf, 21.
[138] *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation*, 57.

security experts lamented that a lack of focus on the encryption of and proper access control to data but the encryption of systems reflected another management misdirection from the agency.[139] Coincidentally, while the House report found that exfiltrated OPM's data using encrypted .RAR files over a months-long span, OPM did not employ the same techniques to safeguard their own data records.

3.3 In Context: Historical OPM Cybersecurity Preparedness and Posture

From 2007 to the present, OPM's Office of the Inspector General has audited the agency's FISMA (Federal Information Security Management Act of 2002, amended in 2014 as the Federal Information Security Modernization Act) compliance. FISMA, first signed into law in Title III of the 2002 E-Government Act as the Federal Information Security Management Act and updated as the Federal Information Security Modernization Act in 2014. Specifically, FISMA "requires (1) annual agency program reviews, (2) annual Inspector General (IG) evaluations, (3) agency reporting to the Office of Management and Budget (OMB) the results of IG evaluations for unclassified systems, and (4) an annual OMB report to Congress summarizing the material received from agencies."[140] From 2007 to 2017, the OPM OIG issued a total of 287 recommendations. An aggregate analysis of the OIG's publicly available, historical audit findings and recommendations from 2007 to 2017 shows two distinct periods in the recommendation data. The first period saw steady growth, then a peak, and a decline in information security-related deficiency findings recommendations in the first period from 2007 to 2013. This trend was followed by a second period of a steadily high rate of recommendations in the OIG reports.[141]

---

[139] *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation*,49-50.
[140] U.S. Office of Personnel Management, Office of the Inspector General, Office of Audits, "Federal Information Security Management Act Audit FY 2007," 4A-CI-00-07-007 (September 18, 2007): 1.
[141] Specific data are available in Appendix II.

Beginning with nine information-security related findings and recommendations in 2007, the OPM OIG issued a record high of 41 recommendations related to FISMA compliance to the agency in 2010. The number of findings and recommendations tapered off consistent in the subsequent years, until hitting a low of 16 in 2013. Beginning in 2014 (with 29 recommendations) to the present (the last OPM OIG FISMA report, released in 2017, contained 39 recommendations for the agency), the OIG consistently found issues with OPM's security posture and made topical recommendations accordingly. The OPM breaches occurred between 2014 and 2015, so it is important to note that while FISMA recommendations and FISMA findings were above-average (with 29 and 27 recommendations made in those respective years), the audits conducted in those two years were by no means the most recommendation-heavy. Perhaps this pattern signals that both OPM leadership and the auditors in the OIG believed that certain information security weaknesses were adequately addressed, only to face one of the biggest cyberattacks in the U.S. federal government's history.

These 287 recommendations spanned 12 categories, including: 1) Agency Privacy Program (20, or 7% of all 287 recommendations); 2) Configuration Management; (68, or 24% of the total); 3) Contingency Planning (24, or 8%); 4) Contractor Systems (10, or 3%); 5) Identity, Credential, and Access Management (29, or 10%); 6) Incident Response Program (11, or 4%); 7) Information Security Continuous Monitoring (18, or 6%); 8) Information Security Governance (23, or 8%); 9) Plan of Action and Milestones (26, or 9%); 10) Risk Management (23, or 8%); 11) Security Assessment and Authorization; (26, or 9%) and 12) Security Training (9, or 3%).[142]

[142] These 10 recommendation categories were found based on the latest nomenclature used by the OPM OIG in the annual OPM FISMA audits from 2007 to 2017. "Agency Privacy Program" includes follow-up recommendations related to the privacy of personally identifiable information and the implementation of OMB M-06-15, which aimed to outline the requirements of a privacy program across different federal agencies. "Configuration Management" includes security configuration management, quality of system inventory, and system inventory-related recommendations and follow-ups. "Contingency Planning" was a consistently-used category historically in OIG reports. "Identity, Credential, and Access Management" roll up the previous nomenclature used in related

Many of these recommendations persisted over time, signaling that OPM took at least a year to address information security issues found by the OIG. 132--nearly half--of the recommendations made since 2007 by the OPM OIG were roll-forward recommendations that carried forward from a previous OIG audit or a series of past OIG audits. 155 of these 287 total recommendations (54%) were actually new recommendations made during the 2007 to 2017 audit timeframe.

Another measure of the integration of information security and cybersecurity thinking in an agency is how quickly they implement the recommendations contained in these FISMA reports. For all 287 recommendations made in the set, each recommendation has an average life of approximately 2.79 years. The average lifespan of a recommendation drops to 1.74 years when considering only the 155 unique, new recommendations per report year. Of the 155 unique recommendations from 2007 to 2017, a total of 116 have been closed, taking an average of 1.52 years to close each recommendation. 39 unique recommendations remain open for OPM to implement; these recommendations are on average slightly over two years old. A graphic of the total recommendations over time is provided on the next page.

recommendations: OPM's account and identity management program, identity and access management, E-authentication risk assessments, and remote access management. This category also focuses on contractor credentials, which also includes previous recommendations related to agency oversight of contract systems as well as OPM's specific program to oversee contractor systems. "Information Security Governance" also refers to security and policies and procedures review and update. "Risk Management" was a subcategory in earlier recommendations previously categorized under agency oversight of contractor systems and the quality of system inventory but fall under OPM's contemporary definitions of risk management. Additionally, the agency plan of action and milestones process is included in this category. "Security Assessment and Authorization" is a category that also includes the testing of security controls. Finally, "Security Management" is a category that also rolls up security awareness training recommendations from previous reports. These ten categories are explained in more detail later in this section of the thesis. The specific insights regarding recommendations and recommendation categories were collected from the OPM OIG's FISMA audit findings and recommendations for each fiscal year from 2007 to 2017. Aggregated data are available in Appendix II.

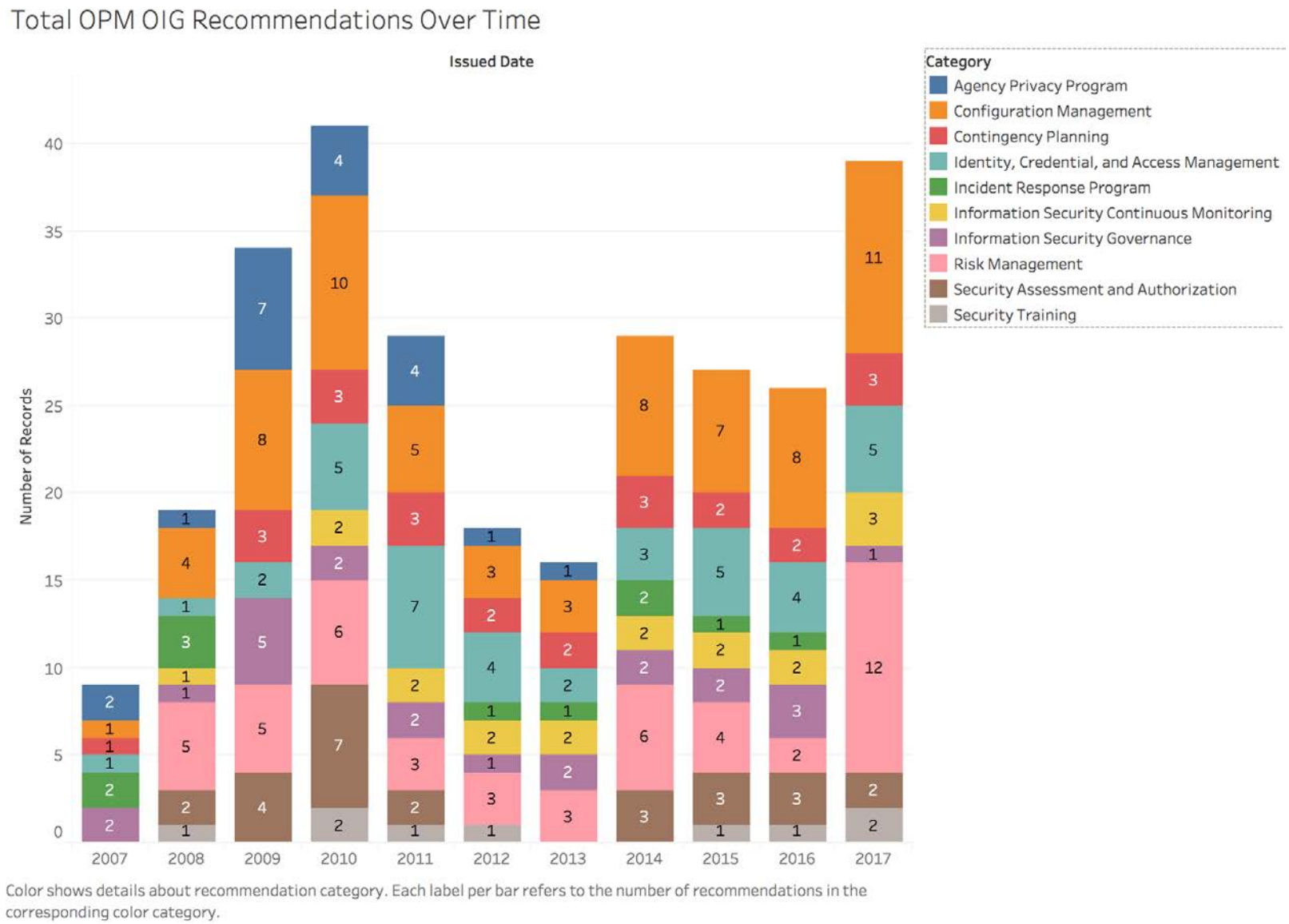


Figure 2. OPM Office of the Inspector General (OIG) FISMA Audit Recommendation Categories, 2007-2017

Interestingly, closed, unique recommendations outnumber open, unique recommendations by almost a factor of three to one. On average, however, it has taken less time to implement these same closed recommendations given by the OIG than the remaining, open ones. The OIG has issued several recommendations that have remained open for a disproportionate amount of time, suggesting specific historical weaknesses in OPM's cybersecurity preparedness in those recommendation areas. If the number of FISMA audit recommendations can be assumed to be a proxy by which the public can measure OPM's security preparedness in the years following the breach, two possible insights emerge. First, auditors in the OIG, cognizant of the cybersecurity weaknesses that led to the breaches may have more heavily scrutinized OPM's information security preparedness after incident and uncovered more problems that were not there before. Secondly, based on OPM's FISMA audit performance in the years following the breaches to their systems, the agency's historical information security and cybersecurity weaknesses still have not been adequately addressed.

3.3.1. Agency Privacy Program

OPM's Agency Privacy Program audit by the OIG included an evaluation of OPM's privacy impact assessment process and its privacy program's progress in implementing OMB Memorandum M-06-15. Privacy impact assessments (PIAs) have been required of any federal agencies that process personally identifiable information (PII). OMB Memorandum M-06-15 "requires agencies to review the administrative, technical, and physical safeguards that protect PII."[143] The OIG issued a total of 20 (7% of the 287 total) recommendations related to OPM's agency privacy program from 2007 to 2017. Of those 20, 11 were new recommendations over the course of the recommendations dataset, and nine of the recommendations rolled forward.

[143] "Federal Information Security Management Act Audit FY 2007," 8.

OPM audit reports indicate that the first agency privacy program recommendations were made in 2007. For the most part, concerns with OPM's privacy program peaked in 2009, with give recommendations. Aside from three recommendations made in 2011, no new recommendations have been made about the agency privacy program since that year. OPM performed the strongest in its agency privacy program, as all recommendations have been marked closed since 2014. On average, OPM took 1.84 years to close these recommendations.

3.3.2. Configuration Management

Configuration management allows organizations to establish system baseline standards, securely manage changes to configuration settings, and monitor system software across the organization. For OPM, configuration management involves developing and maintaining "baseline [federal information technology] configurations and approved standard configuration settings for its information systems."[144] Within the latest OPM OIG report, configuration management findings were an extensive look into the state of OPM's IT infrastructure preparedness and involved several metrics, including configuration management roles, responsibilities, and resources; developing configuration management plans; implementation of policies and procedures; baseline configurations; security configuration settings; flaw remediation and patch management; the trusted internet connection program; and configuration control management.[145]

Configuration management has historically been a weakness for OPM to handle. Over the 2007 to 2017 period, the OIG issued 68 total recommendations related to configuration management to OPM. Related findings and recommendations were the most often made across unique recommendations by the OIG, with 34 unique recommendations (22% of the 155 unique

[144] "Federal Information Security Modernization Act Audit Fiscal Year 2017," ii.
[145] Ibid., 24-31.

recommendations) from 2007 to 2017. The other 34 were rolled over during the timespan. Each year contained at least one new configuration management-related recommendation. The most number of configuration management recommendations made by the OIG was six, in both 2009 and 2014. Of these 34 recommendations, 23 (slightly over two-thirds) have been closed since they were open, each taking an average of 1.64 years to implement.

However, on average, the 11 remaining recommendations have stayed open for an average of slightly over two years. Five of the 11 recommendations are from the 2014 OIG FISMA audit and are tied as the longest roll-forward recommendations in the configuration management category, having each been open for more than three years. These recommendations include priorities such as developing and implementing standard configuration settings for all operating systems platforms in use by OPM, conducting routine compliance scans for all OPM servers and databases, ensuring routine vulnerability scanning on all OPM network-connected devices, tracking security weaknesses during vulnerability scans, and applying operating systems and third-party vendor patches in a timely manner. Most recently, the OIG has noted that OPM has also been "working to establish routine audit processes to ensure that its systems maintain compliance with established configurations."[146]

3.3.3. Contingency Planning

Contingency planning enables organizations to ensure the "adequate availability" of information systems, data, and business processes. FISMA contingency planning requirements include contingency planning roles and responsibilities, contingency planning policies and procedures, business impact analysis, contingency plan maintenance, contingency plan testing, information system backup and storage, communication of recovery activities.[147] The OIG

[146] "Federal Information Security Modernization Act Audit Fiscal Year 2017," ii.
[147] Ibid., 46-50

found that OPM has not implemented FISMA contingency planning recommendations, "and continues to struggle" with such recommendations on a routine basis.[148]

According to the dataset, the OIG issued 24 total contingency planning-related recommendations to OPM from 2007 to 2017. Of these 24, OPM was only given nine unique recommendations (roughly 6% of new recommendations year-over-year from the OIG) on contingency planning over the past ten years. OPM has made significant progress in implementing these nine recommendations, having closed six in an average of 1.8 years per recommendation. The three open recommendations in the contingency planning category include testing contingency plans for each OPM systems annually, ensuring that all of OPM's systems actually have contingency plans in place, and incorporating business impact analysis into the results of system-level contingency plans. The oldest roll-forward recommendation dates from November 2012 and has been open for over five years; this recommendation calls for OPM to simply test contingency plans for each systems it owns on an annual basis. As the OIG concludes, "OPM's failure to test the contingency plans for almost 90 percent of its systems is a symptom of the significant deficiency in the agency's information security governance structure."[149]

3.3.4. Identity, Credential, and Access Management (ICAM)

Identity, credential, and access management (ICAM) is a "Government-wide effort to help Federal agencies provision access to systems and facilities for the right person, at the right time, for the right reason."[150] ICAM efforts do not explicitly target contractor access, as they seek to establish broader guidelines for system permissions of all users of federal IT systems, focusing on the people, processes, and technology related to the digital enterprise. The ICAM

[148] "Federal Information Security Modernization Act Audit Fiscal Year 2017," ii.
[149] Ibid., 46.
[150] Ibid., 31.

category includes the subcategories of assigning personnel risk, defining access agreements for privileged users on OPM-affiliated systems, multi-factor authentication with PIV, strong authentication mechanisms for privileged users, management of privileged user accounts, current and former employee information access, and contractor access management.

ICAM-related recommendations form a significant subset of the total recommendations made from 2007 to 2017 (39 of 287, or 14%) and constitute a similar portion of the unique recommendations made from 2007 to 2017 (22 of 155, or 14%). The total number in this category rank third in the set of all recommendations and the set of all unique recommendations issued by the OPM from 2007 to 2017. Including roll-forwards, 17 ICAM-related recommendations have been closed since 2007, each taking roughly an average of 1.3 years each to close. The five remaining have been open for at least 1.6 years, on average. Two weaknesses in these five remaining recommendations stand out: multi-factor authentication to access major information systems and keeping track of contractors with access to OPM's systems. The longest open recommendation was first issued in 2012 and recommends that OPM require multi-factor authentication using PIV credentials. The second-longest open recommendation was first issued in 2016 and calls for OPM's OCIO to maintain a centralized list of contractors that have access to OPM's network and routinely audit the user accounts on the list.

As of the 2017 FISMA audit, the OIG has not issued any specific contractor management-related recommendations and OPM has been "ensuring that an auditing process is implemented for all contractor access."[151] However, managing contractor systems has been a historical weakness for OPM since at least 2007. Not only do FISMA requirements pertain to agency-owned IT systems and resources, but they also pertain to "IT resources owned and/or

[151] "Federal Information Security Modernization Act Audit Fiscal Year 2017," ii.

operated by a contractor support agency systems."[152] In 2016, the OPM OIG noted that "several information security agreements and memoranda of understanding between OPM and contractor-operated information systems have expired,"[153] pointing to a weakness in the management of contractors by the agency. On paper, however, it seems that OPM's efforts to curb issues in contractor systems have been largely successful. Historically, the OIG has only made 10 overall recommendations (3% of the 287 total) and five unique recommendations (3% of the 155 total unique) pertaining to the sub-category of contractor systems. All five of these unique recommendations have been closed as of 2017, taking an average of 0.86 years to close.

Looking more closely, the longest of these contractor systems recommendations originated from the 2009 OIG report and was rolled forward until the 2011 OIG report. OPM spent two years to develop a policy for adequate oversight of contractor-operated systems. Another outlier was a recommendation related to identifying agency systems residing in a public cloud and including those systems in a master system inventory; this recommendation was made in the 2014 OIG and was marked closed immediately upon publication. OPM's performance in the contractor systems category appears better in the reports than in real life. OPM's specific contractor system compliance outlook improved just as it was being breached via contractor access, suggesting that perhaps this piece fell through the cracks of the FISMA auditing process as the agency geared towards broader focus on access management. As part of a multi-stage cyber espionage operation, adversaries were only able to access OPM's employee data, background check database, and fingerprint records by gaining unauthorized access through KeyPoint contractor credentials. Better managing contractor systems and contractor

[152] U.S. Office of Personnel Management, Office of the Inspector General, Office of Audits, "Federal Information Security Modernization Act Audit Fiscal Year 2016," 4A-CI-00-16-039 (November 9, 2016): 1.
[153] Ibid., ii.

access will remain crucial as part of OPM's security efforts moving forward. Thus, OPM's historical weaknesses specific to contractor systems still largely remain as it grapples with strengthening access management in general.

3.3.5. Incident Response Program

Incident response programs help organizations detect cybersecurity incidents, minimize loss and destruction in such incidents, mitigating exploited vulnerabilities, and restoring availability of IT services.[154] OPM's incident response program reflects a whole-of-government approach in approaching cyber incidents, as FISMA requires federal agencies to establish incident response programs and also requires civilian federal agencies to contact the U.S. Computer Emergency Readiness Team (US-CERT) to "report all incidents consistent with the agency's incident response policy."[155] US-CERT, rolled into the National Cybersecurity and Communications Integration Center (NCCIC), housed within the U.S. Department of Homeland Security, aims to "reduce the risk of systemic cybersecurity and communications challenges" by serving "as a national hub for cyber and communications information, technical expertise, and operational integration, and by operating [the NCCIC] 24/7 situational awareness, analysis, and incident response center."[156] OPM has been successful in implementing an incident response plan, having no open recommendations in the category in the OIG's latest report. Historically, OPM was issued 11 total recommendations (4% of the 287 total), with nine of them unique recommendations over the years (6% of the 155 unique total). The earliest concerns from the OIG on OPM's incident response was 2007, with two recommendations, but by 2017, OPM had

[154] U.S. Department of Homeland Security, Office of Inspector General, *Management Advisory Report: A Guide for Assessing Cybersecurity within the Office of Inspector General Community,* OIG-14-43. February 2014, https://www.ignet.gov/sites/default/files/files/Cybersecurity%20Assessment%20-%20Feb%202014.pdf, 16.
[155] Ibid.
[156] U.S. Department of Homeland Security, United States Computer Emergency Readiness Team, "About Us," *US-CERT*, https://www.us-cert.gov/about-us.

closed all open recommendations made in the category, taking an average of less than a year to close each recommendation. The OIG's concerns mainly centered around internal notification of IT security incidents by employees and contractors, channeling these incident reports upward to OPM leadership, logging, efforts to monitor security events, and building tools to optimize the collection of relevant data for incident response. Indeed, the OIG noted in 2017 that "OPM has an effective incident response program."[157]

3.3.6. Information Security Continuous Monitoring

Information security continuous monitoring (ISCM) involves "the ongoing assessment of the effectiveness of information security controls in support of [OPM's] efforts to manage security vulnerabilities and threats."[158] The ISCM process involves security controls testing and monitoring, processes for ongoing security control assessments and system authorizations, and identifying and defining what constitute effective performance measures for ISCM. From 2007 to 2017, OPM was issued 18 ISCM-related recommendations by the OIG (6% of the 287 total). 12 of these 18 recommendations were unique, meaning six were roll-forward recommendations. The first of these was issued in 2008, and the latest two in this category were issued in 2017. Nine of the unique recommendations were closed over the course of 2011 to 2017, taking an average of almost 0.9 years to satisfy OIG concerns. However, the three open ISCM-related recommendations have been open for an average of almost 3.5 years, nearly four times as long as the time it took for OPM to implement solutions for the closed recommendations. The chief culprit among these open recommendations is a recommendation dating back from 2008. In the 2008 FISMA audit, the OIG recommended that OPM test security controls for all of its systems on an annual basis, and in the nine-and-a-half-year since, the agency still has not closed this

[157] "Federal Information Security Modernization Act Audit Fiscal Year 2017," 44.
[158] Ibid., 40.

recommendation. Unfortunately, ISCM has not been a strong suit for the agency, as the OIG writes in 2017, "OPM must consistently test its systems' security before it can implement a mature continuous monitoring program."[159]

3.3.7. Information Security Governance

Information security governance primarily focuses on "identifying key roles and responsibilities and managing information security policy development, oversight, and ongoing monitoring activities."[160] From 2007 to 2013, the OPM Inspector General found that information security governance was a "material weakness" within OPM. While OPM centralized a cybersecurity program under a Chief Information Security Officer (CISO) in the intervening years between 2013 and 2017, it continued to struggle to implement FISMA requirements. In fact, the 2017 OIG report noted that "when OPM makes progress in one cybersecurity domain, it does so at the expense of another."[161] Historically, the OIG has issued a total of 23 (8% of 287) recommendations pertaining to OPM's information security governance, starting first in 2007 and continuing with one related recommendation each year through 2017. These 23 recommendations whittle down to 11 (7% of 155) after filtering out roll-forward recommendations. Most (10) of these unique recommendations have been closed by OPM, with the agency taking an average of 2.4 years to close them. The remaining single open recommendation has not seen any progress for nearly 1.4 years since its issue. OPM spent more than four years to implement three of the 10 closed recommendations. In these three recommendations, the OIG saw issues with OPM accurately indicating its security position, with implementing a centralized information security governance structure, and with OPM's CIO developing and regularly publishing up-to-date and comprehensive IT security policies

[159] "Federal Information Security Modernization Act Audit Fiscal Year 2017," 43.
[160] Ibid., 8.
[161] Ibid.

and procedures. Overall, the OIG laments that "OPM is not making substantial progress in implementing prior OIG FISMA recommendations."[162]

3.3.8. Risk Management

Risk management allows OPM to "understand and control risks associated with its IT infrastructure and services."[163] Keeping track of system inventories and system interconnections, managing hardware and software inventories, determining system security categorizations, defining risk policy and strategy, designing an information security architecture, and setting risk management roles, responsibilities, and resources are all part of risk management policies for OPM.[164] This category also includes plan of action and milestones tool use (POA&Ms), conducting system level risk assessments, timely risk communication, and contracting clauses that meet federal and OPM requirements and standards. The OIG has emphasized in the 2017 FISMA audit that OPM does not have a tool to view centralized, enterprise-wide risk information, and, "despite a long history of troubled system development projects, OPM still does not consistent enforce a comprehensive [system development life cycle]."[165] Risk management has remained an issue plaguing OPM's IT systems in the dataset.

In fact, OPM has consistently underperformed in the risk management category in historical OIG findings. More specifically, from the total of 49 risk management-related recommendations (17% of 287, or nearly one-fifth), 28 of those 49 are unique recommendations year-over-year (18% of 155, also nearly one-fifth). Risk management is the second-highest occurring recommendation category in the OIG's FISMA audits. Between 2007 to 2017, OPM has only closed 16 (just over half) of these recommendations, taking 1.66 years on average. Of

[162] "Federal Information Security Modernization Act Audit Fiscal Year 2017," 8.
[163] Ibid.,12.
[164] Ibid., 12-19
[165] Ibid., 22.

the 12 remaining open recommendations, six were issued in 2017. However, this subset of recommendations has been open for so long that on average, risk management issues have remained open for nearly two years. The oldest open recommendation was first issued in 2011, and the second oldest was first issued in 2013. The former recommendation involves OPM continuing to develop its risk executive function, while the latter urges OPM to develop a plan and timeline to enforce a new system development lifecycle policy on all development projects to avoid technical issues. Furthermore, these 12 open recommendations actually constitute the biggest subset (31%) of the 39 unique, open recommendations issued from 2007 to 2017. Put simply, a lack of attention to risk management within OPM has certainly exposed the organization to more risk from improper usage and intrusions.

The plan of action and milestones (POA&M) tool comprises a significant part of the risk management process. A POA&M "is a tool used to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of correct efforts for IT security weaknesses."[166] According to the OPM OIG, POA&Ms "incorporate all known IT security weaknesses," prioritize addressing significant IT security weaknesses, call for effective remediation plans as well as adherence to remediation deadlines, identify resources to remediate weaknesses, and include documentation or "proof of closure" indicating that a specific IT weakness has been resolved.[167] As of 2017, OPM has closed all recommendations in POA&M-related sub-categories. In general, however, POA&M-related recommendations have also historically been an OPM weakness, with a total of 26 issued by the OIG (9% of 287) and 14 of the 26 (9% of 155) being unique recommendations that have taken, on average, 1.75 years to implement.

[166] "Federal Information Security Modernization Act Audit FY 2015," 26.
[167] "Federal Information Security Modernization Act Audit Fiscal Year 2017," 26-28.

Four of these POA&M-related recommendations each took OPM three years or more to close. These four recommendations (and associated time to implementation) were in response to the following three issues found by the OIG: (1) that the OPM OCIO and program offices with information systems were not incorporating security weaknesses into appropriate POA&Ms (an issue actually discovered twice--once in 2008 and closed in 2011, another time in 2012 and closed in 2016); (2) that the OPM OCIO and system owners not develop formal action plans to remediate POA&M weaknesses (taking 3.1 years to implement); and (3) and that each IT system owner neither had had an up-to-date POA&M nor regularly submitted an updated POA&M for corresponding systems in OPM's inventory (taking 3.1 years to resolve). The last POA&M-related recommendation was closed in 2016, but two new POA&M recommendations were issued by the OIG in the latest FISMA audit.

3.3.9. Security Assessment and Authorization

Security assessment and authorization is required by both OPM policy and National Institute of Standards and Technology (NIST) guidance. This category in the FISMA audit involves a comprehensive assessment of whether a system's security controls meet requirements and "an attestation that the system risks are at an acceptable level."[168] The OIG noted that while "[p]revious FISMA audits identified a material weakness in OPM's Authorization process related to incomplete, inconsistent, and sub-par work products"[169] and that OPM had worked to resolve some of those same issues, the watchdog ultimately "reinstated the material weakness related to this issue in [the] FY 2015 FISMA audit."[170] While OPM has made some improvements in the authorization process for its systems, issues remain.

[168] "Federal Information Security Modernization Act Audit Fiscal Year 2017," 10.
[169] Ibid.
[170] Ibid.

As the OIG warns, "The lack of an Authorization can indicate that security controls are not operating effectively or that there are unacceptable levels of risk in a system."[171]

Between 2007 to 2017, the OIG issued 26 security assessment and authorization-related recommendations (9% of the 287 total). Of those 26, 12 are unique recommendations that were not roll-forward recommendations (8% of the 155 unique). With 10 of these recommendations now closed (the earliest in 2009, the latest in 2017), two open recommendations in the category remain. OPM indeed made progress on these recommendations between 2009 to 2012, closing a total of nine recommendations in that timespan. However, the two remaining open recommendations have been open for an average of 3.38 years. Both of these recommendations were issued in 2014. One centers around the certification and accreditation (C&A) process of IT systems. The other involves specific authorization errors first identified in 2011 but later brought up in 2014. Overall, open recommendations in the security assessment and authorization category are the second worst-performing, after the information security continuous monitoring category.

3.3.10. Security Training

OPM earned good marks from the OIG for its security training program. FISMA requires all government employees and contractors to undergo IT security training annually and requires IT security-specific employees to take specialized training related to their job function.[172] Furthermore, the OIG notes that "OPM has a strong history of providing its employees with IT security awareness training for the ever changing risk environment and has made progress in providing tailored training to those with significant security responsibilities."[173] Security training involves dedicated policies and procedures, ways to assess

[171] "Federal Information Security Modernization Act Audit Fiscal Year 2017," 11.
[172] Ibid., 37.
[173] Ibid.

the "knowledge, skills and abilities of its workforce" training needs,[174] security awareness strategy, specialized security training policies, and tracking both general and specialized IT security training.

Over the years, the OIG has issued OPM a total of nine security training-related recommendations (3% of 287 total). Of those nine recommendations, seven have been unique recommendations not rolled-forward from previous years. Five of the seven unique recommendations have been implemented by OPM in an average of 1.19 years. The remaining two open recommendations are from the 2017 OIG FISMA audit and involve conducting assessments of workforce security awareness and developing a more tailored security awareness and training strategy. However, with over 96% of OPM employees and contractors having completed security awareness training, the agency has demonstrated sure progress in completing various training requirements.[175]

3.3.11. Current Open Recommendations

Despite the Office of Personnel Management's historical weaknesses in information security, changes promulgated in the years following the OPM data breaches have still not significantly improved the agency's cybersecurity efforts. According to the OPM Office of the Inspector General (OIG), which issues semi-annual reports to Congress on agency compliance, as of September 30, 2017, there were 214 outstanding policy recommendations that were yet to be implemented.[176] These 214 recommendations were made across 50 reports consisting of six types: (1) Internal Operations Audits; (2) Information Systems Audits; (3) Experience-Rated

[174] "Federal Information Security Modernization Act Audit Fiscal Year 2017," 37.
[175] Ibid.
[176] U.S. Office of Personnel Management Office of the Inspector General, "Open Recommendations Over Six Months Old as of September 30, 2017" (December 1, 2017): i.

Insurance Audits; (4) Community-Rated Insurance Audits; (5) Combined Federal Campaign Audits; and (6) Evaluations.[177]

Based on the performance of OPM in accordance to OIG information security audits, information technology remains a lesser priority for the organization. Recommendations from the "Information Systems Audits" category comprised a disproportionate number: 107 (50%) of the 214 total outstanding recommendations. All 107 of these unimplemented recommendations fall under the 188 recommendations that OPM and OIG consider to be procedural recommendations rather than monetary recommendations. Furthermore, from the 214 total recommendations, the remaining 26 monetary recommendations have encompassed an estimated total cost savings of $193,730,170, potentially signaling the organizational priority of OPM when carrying out implementation post OIG reports.[178] If the second-order or even third-order savings from carrying out procedural recommendations could be calculated, the valuation of cost savings from implementing information security and cybersecurity-related recommendations would arguably increase.

Of the 107 outstanding Information Systems Audits recommendations, 70 (65%) relate to Federal Information Security Modernization Act (FISMA) audits. Contemporary FISMA audits review the information security posture of various agencies according to the U.S. Department of Homeland Security's (DHS) FISMA Inspector General Reporting Metrics.[179] Internal documents of OPM's information systems remain confidential and out of public reach, so analyzing the performance of OPM with regards to the OIG FISMA audits gauges the historical performance of OPM in accordance to federally mandated standards of information security. A majority (52

[177] "Open Recommendations Over Six Months Old as of September 30, 2017," i.
[178] Ibid.
[179] "Federal Information Security Modernization Act Audit Fiscal Year 2017," i.

of these 70) of these open FISMA recommendations were made between fiscal year 2014 to fiscal year 2016.[180]

3.4. Evaluation of Technical, Management, and Compliance Factors

In the years leading up to the OPM data breaches, the agency struggled with its fair share of technical issues and management difficulties. OPM failed to detect the technical elements of the incidents, including the specific malware infections and the communications it had with command and control infrastructure until several months after it was initially infected, after tens of millions of records were already exfiltrated. However, as the timeline in the previous chapter demonstrates, OPM was quick to remedy the intrusions with the help of US-CERT after the breaches were detected. This sequence of events suggests that at the time, OPM had greater weaknesses in the detection aspect of the defensive cybersecurity model, but more prowess in the containment and decontamination parts.

On the management side, OPM's lack of IT expertise within its leadership caused it to miss earlier warnings of potential breaches, including the breaches of its closest contractors in investigative services and healthcare. Despite having a directive to implement PIV cards as part of the login process, the agency did not adequately implement multi-factor authentication until months after the attackers' initial entry. Multi-factor authentication would have prevented a critical stolen contractor credential from being used in gaining access to the rest of OPM's servers. Moreover, as a matter of management, OPM neither consistently stored its data within its own premises nor did it encrypt all of its systems.

OPM's FISMA compliance history from 2007 to 2017 gives more weight to the narrative that the agency faced more management mishaps than technical troubles. Countless

[180] "Federal Information Security Modernization Act Audit Fiscal Year 2017," 32-66.

information security-related recommendations from the OPM Inspector General had rolled-forward for several years, indicating management issues in areas of system configuration management; identity, credential, and access management; and risk management. The longest such open recommendation was first issued in September 2008 and recommends OPM to "ensure that an annual test of security controls has been completed for all systems." The multi-factor authentication issue has re-emerged in recent OIG reports, with a recommendation from November 2012 recommending the agency to upgrade its major information systems to require multi-factor authentication using PIV credentials still open to this day. Lastly, despite a change in leadership, OPM's management remains unable to test contingency plans for each of the agency's systems on an annual basis, a finding that has persisted for nearly five-and-a-half years as of this paper's printing. These findings are not prohibitively expensive to implement, nor are they technically challenging. Rather, the narrative that emerges from this compliance history, coupled with the technical and management details from the fact patterns discussed earlier, demonstrates that a lack of prioritization of information security measures from OPM's leadership and management cascaded over time into greater problems that ultimately enabled the intruders to hit the "mother lode."

Today, OPM's management woes extend are seen by entities other than its Inspector General. According to a Government Accountability Office report on OPM's information security posture released in August, 2017, while OPM "has improved its security posture and is in the process of taking numerous actions, such as addressing recommendations from US-CERT and implementing government-wide requirements and initiatives that could decrease the risk of future security breaches if effectively implemented."[181] Its improvements are spotty: OPM

[181] U.S. Government Accountability Office, *Information Security: OPM Has Improved Controls, but Further Efforts are Needed*, GAO-17-614, Washington, D.C., August 2017, https://www.gao.gov/assets/690/686400.pdf, 27.

has not conducted periodic control assessments, has not ensured proper training on the use of monitoring tools, and not comprehensively tested security controls on even a select set of contractor systems.[182] If OPM cannot even play "catch-up" game on information security compliance nearly three years after the 2015 data breaches, how can it expect to keep up with the ever-evolving world of online threat actors?

[182] *Information Security: OPM Has Improved Controls, but Further Efforts are Needed.*

Part Four: Lessons Learned and Future Recommendations

Having triaged the technical and management factors that contributed to the OPM data breaches, this paper now (1) looks at the short-term impacts of the breaches; (2) examines the long-term implications; (3) provides a brief overview of recent U.S. federal government efforts to improve cybersecurity; and (4) offers recommendations based on the lessons learned to improve OPM's future cybersecurity preparedness.

4.1. Short-Term Impact of the OPM Data Breaches

The short-term impact of the OPM data breaches were threefold. First, over 30 million total records were lost, between current and former personnel data, background investigation information, and fingerprints. However, whether those records lost contained specific intelligence community PII remains unknown, as the publicly available paper trail ends with the OPM losses. Second, the immediate political ramifications resulted in a shakeup of leadership. Former OPM Director Katherine Archuleta resigned in June 2015 and, a few months later, Donna Seymore, then-CIO of OPM, resigned in February 2016. These high-level leadership departures would later result in a revolving door of leadership not addressed until nearly three years later. Third, there were also short-term international relations impacts as the U.S. government began the attribution process, linking the OPM breaches to cyber actors associated with the Chinese government.

4.1.1. Lost Data

On June 4, 2015, OPM announced that the personnel data of approximately 4.2 million current and former federal employees were compromised in a cyber incident discovered earlier that year and offered to provide "credit report access, credit monitoring, and identity theft insurance and recovery services to potentially affected individuals" for the following 18

months.[183] Five days later, OPM announced that an incident from late May, 2015, resulted in a breach of the sensitive background investigation information of 21.5 million individuals, including Social Security Numbers, residency and education history, employment history, criminal, and financial history, among many other highly sensitive personal details.[184] Of the 21.5 million records stolen, 19.7 million records contained data of "current, former, and prospective employees and contractors *who applied for a background investigation* in 2000 and after."[185] The other 1.8 million records were of non-applicants "married or otherwise cohabitating with background investigation applications."[186] Furthermore, in September 2015, OPM confirmed the loss of 5.6 million fingerprint record, five times as many records as previously thought.[187]

In fiscal year 2014, OPM began working with the intelligence community's National Counterintelligence and Security Center's (NCSC) Special Security Directorate (SSD) to compile and process data from the Office of National Intelligence's (ODNI) "Scattered Castles" (SC) repository; the Department of Defense's Joint Personnel Adjudication System (JPAS); and OPM's Central Verification System. OPM and the intelligence community collaborated to upload "active, completed clearance records from CVS to SC."[188] Despite worry by security professionals that the SC database, which contains extremely sensitive intelligence community PII, would be similarly compromised, U.S. officials have not confirmed nor denied that the link

[183] "OPM to Notify Employees of Cybersecurity Incident."
[184] U.S. Office of Personnel Management, Office of Communications, "OPM Announces Steps to Protect Federal Workers and Others from Cyber Threats," *OPM.gov*, June 9, 2015, https://www.opm.gov/news/releases/2015/07/opm-announces-steps-to-protect-federal-workers-and-others-from-cyber-threats/.
[185] *OPM Data Breach: Personnel Security Background Investigation Data.*
[186] *Cyber Intrusion into U.S. Office of Personnel Management: In Brief*, 2.
[187] Peterson.
[188] U.S. Office of the Director of National Intelligence, "2014 Report on Security Clearance Determinations." *DNI.gov*, April 2015, https://www.dni.gov/files/documents/2015-4-21%20Annual%20Report%20on%20Security%20Clearance%20Determinations.pdf, 3.

between OPM's CVS and ODNI's was bidirectional. Without more publicly available details about SC, it is hard to make a determination as to whether the perpetrators of the OPM breaches did indeed have access to SC while they were inside OPM's systems.

4.1.2. Political Ramifications

Almost immediately after the data breaches were announced publicly, bipartisan criticism emerged over OPM's handling of the incidents. The political ramifications of the OPM data breaches involved a change in leadership at the agency, resulting in a multi-year leadership vacuum following the resignations of Director Archuleta in July 2015 and Chief Information Officer Donna Seymour in February 2016. This leadership vacuum included both the Office of the Director and the Office of the Chief Information Officer.

OPM took almost three years to appoint a permanent successor to Archuleta. Beth Cobert served as Acting Director of OPM from July 2015 until January 19, 2017, near the very end of the Obama administration. Succeeding Cobert was Kathleen McGettigan, who served in the Acting Director role from January 19, 2017 until March 9, 2018, when Jeff Pon, the current permanent Director of OPM, began his tenure. OPM took six months before announcing the replacement CIO to Donna Seymour after her resignation in February, 2016, naming David DeVries to the position in August that August.[189] DeVries would leave OPM only thirteen months later, in September 2017.[190] OPM named its current CIO David Garcia to the position in October, 2017.[191] Notably, both OPM Director Pon and CIO Garcia have some background in

[189] Angus Loten, "OPM Hires Permanent CIO," *The Wall Street Journal*, August 10, 2016, https://blogs.wsj.com/cio/2016/08/10/opm-hires-permanent-cio/.
[190] Kim S. Nash, "Office of Personnel Management CIO to Leave in September," *The Wall Street Journal*, August 10, 2017, https://blogs.wsj.com/cio/2017/08/10/office-of-personnel-management-cio-to-leave-in-september/.
[191] U.S. Office of Personnel Management, Office of Communications, "Statement: OPM names new Chief Information Officer," *OPM.gov*, October 2, 2017, https://www.opm.gov/news/releases/2017/10/statement-opm-names-new-chief-information-officer/.

technology, perhaps forecasting a future in which the cybersecurity conversation remains at the OPM leadership's table.

4.1.3. Monetary Costs

OPM awarded two contracts to two different private firms to provide credit monitoring and identity protection services to victims shortly after notifying them of the breach. For 4.2 million current and federal employees who had their personnel information stolen, OPM awarded a contract worth $20 million to an identity protection firm named CSID to provide 18 months of protection.[192] OPM awarded a $133 million contract to the firm ID Experts to provide credit monitoring to the 21.5 million victims who had their background checks compromised.[193] OPM also requested that the Department of Defense provide up to $132 million to pay for further identity protection and background investigation.[194] In OPM's haste to alert victims and provide protection services, OPM may have both overestimated the cost of identity protection services and failed to consider duplication costs in the case that the same individual's information happened to be in both sets of records.[195]

On paper, with both OPM and DoD shouldering costs, the cost of handling the breach's aftermath totals upwards of $285 million. More pessimistic experts have estimated that the total costs could exceed $1 billion.[196] Such a figure suggests that certain audit methodologies may not properly estimate the risks associated with a cyber breach. Recalling that the OPM OIG's remaining open information technology recommendations would yield an estimated $0 in

[192] Krebs, "OPM (Mis)Spends $133M on Credit Monitoring."
[193] Ibid.
[194] Jason Miller, "DoD's share of the OPM data breach: $132 million., *Federal News Radio*, August 25, 2015, https://federalnewsradio.com/opm-cyber-breach/2015/08/dods-share-opm-data-breach-132-million/.
[195] Nicole Ogrysko, "OPM may have overestimated cost of ID theft services for cyber breach victims," *Federal News Radio*, March 31, 2017, https://federalnewsradio.com/opm-cyber-breach/2017/03/opm-may-overestimated-cost-id-theft-services-cyber-breach-victims/.
[196] Chris Townsend, "OPM Breach Costs Could Exceed $1 Billion," *Symantec Official Blog*, March 23, 2017, https://www.symantec.com/connect/blogs/opm-breach-costs-could-exceed-1-billion.

savings from the OIG's September 30, 2017 report, perhaps future estimates of the cost savings of IT-related recommendations can include the potential costs of second- or third-order effects in the case that they are not implemented, and another major breach occurs.

4.1.4. International Relations Impacts

In the months immediately after news broke of the OPM breaches, many U.S. officials indirectly attributed the incidents to China, while private-sector security researchers were more public with their attribution. For nation-state governments and especially for the United States, the difficulty in attribution lies in its being a balancing act: more attention and resources dedicated to attribution make it easier, but adversaries are catching on, knowing that false flags may be planted. But attribution lies beyond just the technical domain; many nations have the requisite technical forensics capabilities to make an attribution judgment, but uncertainty in attribution is "a political and policy matter rather than a technical one."[197] Given the delicate balancing act between technical certainty and political prudence in attribution, perhaps it was in the context of an upcoming state visit in September 2015 by Chinese President Xi Jinping that drove U.S. policymakers to avoid direct attribution immediately after the fact.

As the Obama administration mulled over its possible options in the wake of the breach,[198] complicating the international relations impact of the breach was the United States' distinction between cyber intrusions for national security purposes (which merits a counterintelligence response) and cyber intrusions for commercial purposes (which the United States would prefer a criminal justice response). On September 25, 2015, during the Chinese state visit, both Presidents Obama and Xi agreed to a deal that would stop cyber espionage between the two countries, including intellectual property, trade secrets, or other confidential

[197] Lin, 45.
[198] David E. Sanger, "U.S. Decides to Retaliate Against China's Hacking," *The New York Times*, July 31, 2015, https://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html?_r=1.

business information.[199] The two Presidents also agreed to establish high-level joint dialogue to fight cybercrime and related issues.[200] A more direct attribution or an escalatory response would have come at the risk of losing the agreement from September 2015. Furthermore, the early December 2015 arrests of the supposed hackers behind the OPM breach by the Chinese government all but confirmed that the OPM breach came from China, direct attributability of the breach to the government notwithstanding.[201]

4.2. Long-Term Implications of the Incidents

4.2.1. Lagging Federal Background Check Performance

Background checks for clearance investigations were temporarily suspended in the aftermath of the 2015 OPM breach, as the agency worked to clean up the results of the breach. After OPM decided to terminate a contractor relationship with USIS, a contractor that then "accounted for 60 percent of the federal government's investigative capacity around background checks,… OPM has been playing catch up ever since."[202]Indeed, since the OPM breach, there has been a growing backlog of incomplete background check investigations. In 2016, OPM reported that there were roughly 570,000 unfinished clearances. As of July, 2017, there were as many as 690,000 incomplete investigations in the backlog. Just a month later, in August, 2017, that backlog grew to more than 700,000.

In fact, as of March 2017, it took an average of 450 days to conclude a top secret security clearance. Worse yet, in a June 15, 2017, memo, the U.S. Office of Management and Budget

[199] Demetri Sevastopulo and Geoff Dyer, "Obama and Xi in deal on cyber espionage," *Financial Times*, September 25, 2015, https://www.ft.com/content/0dbcab36-63be-11e5-a28b-50226830d644.
[200] U.S. Library of Congress, Congressional Research Service, *U.S.-China Cyber Agreement*, by John W. Rollins, IN10376, October 16, 2015, https://fas.org/sgp/crs/row/IN10376.pdf.
[201] Tony Cole, "Attributions and Arrests: Lessons from Chinese Hackers," *FireEye*, December 3, 2015, https://www.fireeye.com/blog/executive-perspective/2015/12/attributions_andarr.html.
[202] Derek B. Johnson, "NBIB confirms 700,000 security clearance backlog," *FCW*, September 6, 2017, https://fcw.com/articles/2017/09/06/nbib-phelan-clearance-backlog.aspx.

discontinued a set of Obama-era reporting standards in a memorandum that made it much more difficult to track OPM's progress in working through its increasing backlog.[203] This backlog will result in a shortage of skilled, young, and cleared contractor or federal employees that would serve elsewhere; may ignite a "talent war" and disrupt government work; and might drive up wages for existing workers who already have security clearances.[204]

4.2.2. Stolen Data Has Not Been Shared or Sold

When news of the OPM breaches first broke, cybersecurity experts feared that the theft of personally identifiable information (PII) would be used for identity theft or other financially motivated cybercrime.[205] In the days after the breach, a database supposedly from the OPM breach containing a user database exclusively of .gov (U.S. government-related) user accounts floated around in cybercrime circles. However, security researchers were quick to debunk such claims. They found that the data leak was from an unrelated cybersecurity incident in September 2013, when UNICOR.gov, a wholly owned United States government corporation also known as Federal Prison industries, discovered unauthorized access to its public website.[206]

Fortunately, over two years afterwards, in September 2017, William Evanina, Director of the U.S. National Counterintelligence and Security Center, reassured the public in an interview with Bloomberg that the millions of data records, including Social Security numbers and fingerprints, from the OPM data breaches have not been "shared or sold by the perpetrators."[207]

---

[203] Aaron Gregg, "Delays in federal background checks leave more than 700,000 people in limbo," *The Washington Post*, August 27, 2017, https://www.washingtonpost.com/business/economy/delays-in-federal-background-checks-leave-more-than-700000-people-in-limboas-backlog-grows-trump-administration-stops-reporting-numbers/2017/08/25/8a1bbab6-8921-11e7-a94f-3139abce39f5_story.html?utm_term=.19227127aba3

[204] Gregg.

[205] *Cyber Intrusion into U.S. Office of Personnel Management: In Brief.*

[206] Brian Krebs, "OPM's Database for Sale? Nope, It Came from Another US .Gov," Krebs on Security, June 18, 2015, https://krebsonsecurity.com/2015/06/opms-database-for-sale-nope-it-came-from-another-us-gov/.

[207] Chris Strohm, "Hacked OPM Data Hasn't Been Shared or Sold, Top Spy-Catcher Says," *Bloomberg*, September 28, 2017, https://www.bloomberg.com/news/articles/2017-09-28/hacked-opm-data-hasn-t-been-shared-or-sold-top-spy-catcher-says.

While Evanina was hesitant to confirm that the cyber incidents originated from China, he was confident that the personally identifiable information had not been otherwise distributed online as no evidence that those pieces of data had been improperly used in the context of cybercrime.

4.2.3. Counterintelligence Implications

While there have been few indications that the records stolen from OPM have been leveraged by the attackers or otherwise exploited, any theft of personally identifiable information from a government source has profound implications for that nation-state's intelligence efforts. For members of the United States intelligence community undercover abroad, having personal details exposed could result in their compromise.

In late September 2015, the Washington Post reported that the Central Intelligence Agency pulled officers from the U.S. Embassy in Beijing as a precautionary measure, as comparing the background checks of State Department employees and cross-referencing those records with embassy personnel could lead to potential CIA officers undercover.[208] Interestingly, in early November, 2015, Director of National Intelligence James Clapper indicated that the CIA did not pull officers from Beijing, directly contradicting previous reports.[209] Despite these inconsistencies, this episode remains a lesson to be learned for counterintelligence implications in the aftermath of the OPM breach. As the tens of millions of records are still out there, the impacts of the breach will nevertheless be a latent concern for the U.S. intelligence community in the years to come.

---

[208] Ellen Nakashima and Adam Goldman, "CIA pulled officers from Beijing after breach of federal personnel records," *The Washington Post*, September 29, 2015, https://www.washingtonpost.com/world/national-security/cia-pulled-officers-from-beijing-after-breach-of-federal-personnel-records/2015/09/29/1f78943c-66d1-11e5-9ef3-fde182507eac_story.html?noredirect=on&utm_term=.754b778d7a55.

[209] Ellen Nakashima and Adam Goldman, "U.S. intelligence head: CIA did not pull officers from Beijing after OPM hack," *The Washington Post*, November 2, 2015, https://www.washingtonpost.com/world/national-security/us-intelligence-head-cia-did-not-pull-officers-from-beijing-after-opm-hack/2015/11/02/8631aa4e-81a5-11e5-a7ca-6ab6ec20f839_story.html?utm_term=.153f8bca34d6.

4.3. Recent Federal Government Cybersecurity Policies

4.3.1. Obama Administration Initiatives

Although OPM's information security posture and preparedness have historically been weak, the U.S. federal government as a whole has attempted to improve its defensive cybersecurity capabilities. In July, 2015, the Obama administration supported private sector efforts to improve cybersecurity; expanded public-private partnerships and efforts in information security; and pushed for legislation on information sharing and breach notification laws. On the federal cybersecurity front, the administration vastly accelerated cybersecurity efforts through the emphasis and adoption of more secure technologies and expanded capabilities; began a cross-agency effort to examine the background investigation process; and sought to improve the development of the workforce in information security matters through the National Initiative for Cybersecurity Education. The administration also took measures to better "identify, defend against, and counter malicious cyber actors" and engage internationally on cybersecurity issues with both global partners and NATO.[210] In February 2016, the Obama administration proposed the Cybersecurity National Action Plan (CNAP) to "near-term actions and puts in place a long-term strategy to enhance cybersecurity awareness and protections, protect privacy, maintain public safety as well as economic and national security, and empower Americans to take better control of their digital security."[211]

[210] The White House, Office of the Press Secretary, "FACT SHEET: Administration Cybersecurity Efforts 2015," *The White House*, July 09, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/07/09/fact-sheet-administration-cybersecurity-efforts-2015.
[211] The White House, Office of the Press Secretary, "FACT SHEET: Cybersecurity National Action Plan," *The White House*, February 9, 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

4.3.2. Trump Administration Continuity

The Trump administration has stayed consistent with the Obama administration in focusing on strengthening the cybersecurity of federal networks and critical infrastructure. In May 2017, President Trump issued an Executive Order 13800 outlining concrete steps to improve cybersecurity. First, the Executive Order requires agency heads to utilize the National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure (completed as a result an Executive Order signed by President Obama in 2013);[212] directs agency heads to produce cybersecurity risk reports to both the leadership of the Department of Homeland Security and the Office of Management and Budget; and prioritizes the policy to "build and maintain a modern, secure, and more resilient executive branch IT architecture."[213] Second, the Executive Order 13800 directs agencies to support the security efforts of critical infrastructure entities at the greatest risk of attacks and mandates investigation and reporting on critical infrastructure threats. Third, focusing on "Cybersecurity for the Nation," Executive Order 13800 directs several executive branch leaders to submit a report on strategic options for cyber deterrence; directs executive branch leaders to submit a report on international cybersecurity priorities; and identify workforce development opportunities to "ensure that the United States maintains a long-term cybersecurity advantage."[214] Unfortunately, as deadlines detailed in the Executive Order approached late last year, the reports directed by Executive Order 13800 failed to materialize, suggesting ambitious goals but lagging efforts from the current administration in the space.[215]

---

[212] Helen Klein Murillo, "A Summary of the Cybersecurity Executive Order," *Lawfare Institute*, May 11, 2017, https://www.lawfareblog.com/summary-cybersecurity-executive-order.
[213] Executive Order No. 13800, 3 C.F.R. 22391 (May 11, 2017), https://www.gpo.gov/fdsys/pkg/FR-2017-05-16/pdf/2017-10004.pdf.
[214] Ibid.
[215] Lily Hay Newman, "Taking Stock of Trump's Cybersecurity Executive Order So Far," *Wired*, September 3, 2017, https://www.wired.com/story/trump-cybersecurity-executive-order/.

4.4. Recommendations for Future Cybersecurity Preparedness

With federal government efforts from the past five years in consideration, the following five recommendations include both near-term efforts to combat immediate problems OPM faces and long-term efforts to improve the agency's cybersecurity strategy overall. They attempt to address many of the structural management issues plaguing OPM while also enhancing the agency's technical capabilities in detecting and mitigating cyber intrusions or cyberattacks.

The first recommendation focuses on the "catch up" game; the second recommendation centers on a continuous-improvement process as suggested by the National Institutes of Standards and Technology's (NIST) cybersecurity framework; the third recommendation seeks to ensure that OPM's contractor relationships have the proper credentials and access management to prevent the possibility of a stolen credential being used in a breach again; the fourth recommendation suggests restructuring information technology security training programs to better verify the training progress of OPM's employees; and finally, the fifth recommendation includes the possibility of developing public-private partnerships to improve OPM's technical capabilities.

Recommendation 1: *Prioritize Implementation of Oldest Open OIG FISMA Recommendations*

> The **Director of OPM** and the **Office of the Chief Information Officer** should work with **all relevant program offices** to prioritize the necessary resources, time, and personnel to implement all Inspector General FISMA audit recommendations that have been **open for two years or more** before the issuance of the OIG's FY 2018 FISMA audit. Prioritizing these 16 open recommendations (as of March 30, 2018) would improve historically problematic recommendation categories for OPM, such as information security continuous monitoring; risk management; and identity, credential, and access management.

Recommendation 2: *Develop Security Best Practices through Continuous Improvement*

The **Director of OPM** and the **Office of the Chief Information Officer** should draft and publish a draft strategy document developing a set of best practices focused on best-demonstrated continuous-improvement processes as documented in the latest revision of the *NIST Framework for Improving Critical Infrastructure Cybersecurity*, including the key functions of **identification** of; **protection** from; **detection** of; **response** to; and **recovery** from cyber espionage, cyber breaches, cyberattack, and other malicious cyber activities, **by the end of FY 2018.**

Recommendation 3*: Evolve the Contractor Relationship*

The **Director of OPM** and **all related program offices** should act to facilitate an evolution in the contractor relationship to better manage the risks associated with contractors providing key services for the agency. These actions should include, as a baseline, improved identity verification; consolidated credential management; and more granular access management. These new policies should be published **by the end of FY 2018** and enacted either **by the end of FY 2018** or the next OPM contractor services agreement following policy publication, **whichever is sooner.**

Recommendation 4: *Restructure IT Security Training Programs*

The **Director of OPM** and the **Office of the Chief Information Officer**, working with **all relevant OPM program offices,** should publish findings on all agency security training efforts, including all cybersecurity-related education curricula, training percentage rates, and training retention; report these findings to the OIG in a timely manner; and develop and restructure IT security training programs accordingly to maximize training effectiveness and concept retention among all OPM employees and contractors.

Recommendation 5: *Develop Public-Private Partnerships for Information Sharing*

The Director of OPM, in a cross-agency effort with all other executive branch offices and FISMA-designated cybersecurity response agencies, should author and publish a report on public-private partnerships for cybersecurity information sharing and incident response within 180 days and develop an actionable timeline for working with the private sector entities identified in the report within 180 days of the report's release.

Conclusion

The OPM data breach was the worst publicly known cyber incident to befall the U.S. federal government in recent memory. The massive losses from the breach--including 4.2 million former and current federal employee personnel records, 21.5 million background checks for national security positions, and 5.6 million sets of fingerprints--stemmed from a sophisticated, multi-stage cyber espionage operation linked to state-sponsored actors. Such a large data breach invited bipartisan criticism of the agency's handling of the incidents and thrust the federal government's cybersecurity preparedness into the limelight.

What happened to OPM was actually a set of cybersecurity breaches from skilled attackers that exploited a combination of technical vulnerabilities present in OPM's systems. These technical weaknesses were only magnified by management woes: a lack of information technology leadership from the agency, missed warning signs, inadequate implementation of technically feasible security measures, poor contractor management, and data management policy issues. Furthermore, a historical analysis of OPM's FISMA compliance from 2007 to 2017 suggest that the agency had lagged behind in implementing many recommendations that could have improved its cybersecurity posture. In fact, the data show that in the years since the OPM breach, the agency's IT security compliance issues have only gotten worse.

In the United States, cybersecurity is an issue that bridges the political divide, with both bipartisan attention paid to the issue and support for the improvement of cybersecurity and IT infrastructure within the Federal government. Both the Obama and Trump administrations have emphasized the importance of strengthening the nation's cybersecurity capabilities to avoid breaches such as the one that befell OPM and have detailed policy initiatives to involve a broad base of stakeholders, including cross-agency efforts and the private sector. Following this trajectory, the recommendations proposed in this thesis are made with the hope that, if

followed, OPM can successfully grapple with its historic information technology management weaknesses, adopt a continuous improvement framework in thinking about cybersecurity, and ensure that future breaches of its sensitive databases never occur again.

Bibliography

"FBI Warns U.S. Businesses of China-backed Cyberattacks." *NBC News*. October 15, 2014. https://www.nbcnews.com/tech/security/fbi-warns-u-s-businesses-china-backed-cyberattacks-n226821.

"PlugX." *NJ Cybersecurity & Communications Integration Cell*. April 12, 2017. https://www.cyber.nj.gov/threat-profiles/trojan-variants/plugx.

"Put up the firewalls: Bureaucratic inertia makes life easy for foreign hackers." *The Economist*. June 11, 2015. https://www.economist.com/news/united-states/21654078-bureaucratic-inertia-makes-life-easy-foreign-hackers-put-up-firewalls.

"Sakula." *NJ Cybersecurity & Communications Integration Cell*. April 26, 2017. https://www.cyber.nj.gov/threat-profiles/trojan-variants/sakula.

"Significant Cyber Incidents." *Center for Strategic and International Studies*. 2018. https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity.

Adams, Michael. "Why the OPM Hack is Far Worse Than You Imagine." *Lawfare Institute*. March 11, 2016. https://www.lawfareblog.com/why-opm-hack-far-worse-you-imagine.

Barrett, Devlin, Danny Yadron, and Damian Paletta. "U.S. Suspects Hackers in China Breached About 4 Million People's Records, Officials Say." *The Wall Street Journal*. June 5, 2015. https://www.wsj.com/articles/u-s-suspects-hackers-in-china-behind-government-data-breach-sources-say-1433451888.

Barrett, Devlin. "Chinese national arrested for allegedly using malware linked to OPM hack." *The Washington Post*. August 24, 2017. https://www.washingtonpost.com/world/national-security/chinese-national-arrested-

for-using-malware-linked-to-opm-hack/2017/08/24/746cbdc2-8931-11e7-a50f-e0d4e6ec070a_story.html?utm_term=.78790efebefc.

Bennett, Brian and W. J. Hennigan. "China and Russia are using hacked data to target U.S. spies, officials say." *Los Angeles Times.* August 31, 2015. http://www.latimes.com/nation/la-na-cyber-spy-20150831-story.html.

Bennett, Cory. "FBI: Chinese malware possibly behind OPM hack." *The Hill*. July 2, 2015. http://thehill.com/policy/cybersecurity/246754-fbi-warns-of-chinese-malware-possibly-behind-opm-hack.

Berliner, Ben. "OPM still plagued by cyber weaknesses, IG finds." *FCW*. November 7, 2017. https://fcw.com/articles/2017/11/07/opm-cyber-fisma-oig.aspx.

Boyd, Aaron. "OPM CIO Seymour resigns days before Oversight hearing." *Federal Times.* February 22, 2016. https://www.federaltimes.com/it-networks/2016/02/22/opm-cio-seymour-resigns-days-before-oversight-hearing/.

Buchanan, Ben. *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations.* New York: Oxford University Press, 2016.

Bur, Jessie. "OPM fails 'open book test' on security." *Fifth Domain*. November 7, 2017. https://www.fifthdomain.com/federal-oversight/2017/11/07/opm-fails-open-book-test-on-security/.

Carollo, Malena. "U.S. retaliation for OPM hack could set precedent in global cyberconflict." *The Christian Science Monitor*. August 21, 2015. https://www.csmonitor.com/World/Passcode/2015/0821/US-retaliation-for-OPM-hack-could-set-precedent-in-global-cyberconflict.

Chalfant, Morgan. "Court dismisses lawsuits over OPM data breach." *The Hill*. September 19, 2017. http://thehill.com/policy/cybersecurity/351395-court-dismisses-lawsuits-over-opm-data-breach.

Chappell, Bill. "Obama: Cyberspace Is the New 'Wild West.'" *NPR*. February 13, 2015. https://www.npr.org/sections/thetwo-way/2015/02/13/385960693/obama-to-urge-companies-to-share-data-on-cyber-threats.

Clapper, James R. "Worldwide Cyber Threats." Statement for the Record, U.S. Cybersecurity and Policy, *Senate Armed Services Committee.* September 29, 2015. https://www.armed-services.senate.gov/imo/media/doc/Clapper_09-29-15.pdf.

Cobert, Beth. "Report on Cyber Intrusions at OPM." U.S. Office of Personnel Management, Director's Blog." *OPM.gov.* September 7, 2016. https://www.opm.gov/blogs/Director/2016/9/7/Report-on-Cyber-Intrusions-at-OPM/.

Cole, Tony. "Attributions and Arrests: Lessons from Chinese Hackers." *FireEye.* December 3, 2015. https://www.fireeye.com/blog/executive-perspective/2015/12/attributions_andarr.html.

Cole, Tony. "Attributions and Arrests: Lessons from Chinese Hackers." *FireEye*. December 3, 2015. https://www.fireeye.com/blog/executive-perspective/2015/12/attributions_andarr.html.

Davis, Julie Hirschfeld. "Katherine Archuleta, Director of Personnel Agency, Resigns." *The New York Times.* July 10, 2015. https://www.nytimes.com/2015/07/11/us/katherine-archuleta-director-of-office-of-personnel-management-resigns.html.

Dell SecureWorks Counter Threat Unit Threat Intelligence. "Sakula Malware Family." *SecureWorks*. July 30, 2015. https://www.secureworks.com/research/sakula-malware-family.

DeNardis, Laura. "Five Destabilizing Trends in Internet Governance." *I/S: A Journal of Law and Policy for the Information Society* 12 (2015): 113-134. http://heinonline.org/HOL/LandingPage?handle=hein.journals/isjlpsoc12&div=11&id=&page=.

FCW Staff. "Revealing the RATs and scoring the agencies." *FCW*. June 29, 2015. https://fcw.com/articles/2015/06/29/news-in-brief-june-29.aspx?s=fcwdaily_300615.

Federal Information Security Modernization Act of 2014. Public Law 113-283. 128 Stat. 3073-3088. December 18, 2014. https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf.

Gallagher, Sean. "'EPIC' fail--how OPM hackers tapped the mother lode of espionage data." *Ars Technica*. June 21, 2015. https://arstechnica.com/information-technology/2015/06/epic-fail-how-opm-hackers-tapped-the-mother-lode-of-espionage-data/.

Gallagher, Sean. "Encryption 'would not have helped' at OPM, says DHS official." *Ars Technica*. June 16, 2015. https://arstechnica.com/information-technology/2015/06/encryption-would-not-have-helped-at-opm-says-dhs-official/.

Gallagher, Sean. "Surprise! House Oversight report blames OPM leadership for breach of records." *Ars Technica*. September 7, 2016. https://arstechnica.com/information-technology/2016/09/surprise-house-oversight-report-blames-opm-leadership-for-breach-of-records/.

Gallagher, Sean. "Why the 'biggest government hack ever' got past the feds." *Ars Technica*. June 8, 2015. https://arstechnica.com/information-technology/2015/06/why-the-biggest-government-hack-ever-got-past-opm-dhs-and-nsa/.

Glyer, Christopher and Ryan Kazanciyan. "The 'Hikit Rootkit: Advanced and Persistent Attack Techniques (Part 2)." *FireEye*. August 22, 2012. https://www.fireeye.com/blog/threat-research/2012/08/hikit-rootkit-advanced-persistent-attack-techniques-part-2.html.

Gregg, Aaron. "Delays in federal background checks leave more than 700,000 people in limbo." *The Washington Post*. August 27, 2017. https://www.washingtonpost.com/business/economy/delays-in-federal-background-checks-leave-more-than-700000-people-in-limboas-backlog-grows-trump-administration-stops-reporting-numbers/2017/08/25/8a1bbab6-8921-11e7-a94f-3139abce39f5_story.html?utm_term=.19227127aba3.

Groll, Elias. "Clapper: 'We Don't Know Exactly What Was Taken in the OPM Breach.'" *Foreign Policy*. September 24, 2015. http://foreignpolicy.com/2015/09/24/clapper-we-dont-know-exactly-what-was-taken-in-the-opm-breach/.

Harris, Shane. "Spies Warned Feds About OPM Mega-Hack Danger." *The Daily Beast*. June 30, 2015. https://www.thedailybeast.com/spies-warned-feds-about-opm-mega-hack-danger.

Hennessey, Susan. "Deterring Cyberattacks: How to Reduce Vulnerability." *Foreign Affairs*. Nov./Dec. 2017. https://www.foreignaffairs.com/reviews/review-essay/2017-10-16/deterring-cyberattacks.

Jervis, Robert. "Cooperation Under the Security Dilemma." *World Politics* 30, no. 2 (January 1978): 167-214. DOI: 10.2307/2009958.

Johnson, Derek B. "NBIB confirms 700,000 security clearance backlog." *FCW*. September 6, 2017. https://fcw.com/articles/2017/09/06/nbib-phelan-clearance-backlog.aspx.

Katz, Eric. "With No Confirmed Director, OPM Could Struggle to Implement Trump's Agenda." *Government Executive*. August 17, 2017. https://www.govexec.com/management/2017/08/no-confirmed-director-opm-could-struggle-implement-trumps-agenda/140332/.

Kennel, David. "OPM vs. APT: How Proper Implementation of Key Controls Could Have Prevented a Disaster." *SANS Institute*. March 10, 2016. https://www.sans.org/reading-room/whitepapers/breaches/opm-vs-apt-proper-implementation-key-controls-prevented-disaster-36852.

Koerner, Brendan I. "Inside the Cyberattack that Shocked the US Government." *Wired*. October 23, 2016. https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/.

Krebs, Brian. "Catching Up on the OPM Breach." *Krebs on Security*. June 15, 2015. https://krebsonsecurity.com/2015/06/catching-up-on-the-opm-breach/.

Krebs, Brian. "OPM (Mis)Spends $133M on Credit Monitoring." *Krebs on Security*. September 2, 2015. https://krebsonsecurity.com/2015/09/opm-misspends-133m-on-credit-monitoring/.

Krebs, Brian. "OPM's Database for Sale? Nope, It Came from Another US .Gov." *Krebs on Security*. June 18, 2015. https://krebsonsecurity.com/2015/06/opms-database-for-sale-nope-it-came-from-another-us-gov/.

Lee, Robert M. and Thomas Rid. "OMG Cyber!: Thirteen Reasons Why Hype Makes for Bad Policy." *The RUSI Journal* 159, no. 5: 4-12 (2014). DOI: 10.1080/03071847.2014.969932. http://www.tandfonline.com/doi/full/10.1080/03071847.2014.969932.

Lin, Herbert. "Attribution of Malicious Cyber Incidents: From Soup to Nuts." *Hoover Institution Aegis Paper Series, no. 1607.* September 19, 2016. https://www.hoover.org/sites/default/files/research/docs/lin_webready.pdf.

Loten, Angus. "OPM CIO Resigns, but Blame for Data Breach Lingers." *The Wall Street Journal.* February 23, 2016. https://blogs.wsj.com/cio/2016/02/23/opm-cio-resigns-but-blame-for-data-breach-lingers/.

Loten, Angus. "OPM Hires Permanent CIO." *The Wall Street Journal*. August 10, 2016. https://blogs.wsj.com/cio/2016/08/10/opm-hires-permanent-cio/.

Mandiant Intelligence Center. "APT1: Exposing One of China's Cyber Espionage Units." *Mandiant*. February 19, 2013. https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

Martemucci, Matteo G. "Offensive Dimensions of Cyber Security: Strategy and Policy Challenges." *U.S. Air Force 318th Cyberspace Operations Group*. August 2014.

Mazmanian, Adam "OPM's sensitive data on feds still not encrypted." *FCW*. May 13, 2016. https://fcw.com/articles/2016/05/13/opm-encryption-legacy.aspx.

Menn, Joseph. "Chinese national arrested in Los Angeles on U.S. hacking charge." *Reuters*. August 24, 2017. https://www.reuters.com/article/us-usa-cyber-opm/chinese-national-arrested-in-los-angeles-on-u-s-hacking-charge-idUSKCN1B42RM.

Michaels, Dave. "SEC Discloses Edgar Corporate Filing System Was Hacked in 2016." *The Wall Street Journal*. September 20, 2017. https://www.wsj.com/articles/sec-discloses-edgar-corporate-filing-system-was-hacked-in-2016-1505956552.

Miller, Jason. "3 years after data breach, OPM still struggling to modernize IT." *Federal News Radio*. February 27, 2018. https://federalnewsradio.com/opm/2018/02/three-years-after-data-breach-opm-still-struggling-to-modernize-its-it/.

Miller, Jason. "DoD's share of the OPM data breach: $132 million." *Federal News Radio*. August 25, 2015. https://federalnewsradio.com/opm-cyber-breach/2015/08/dods-share-opm-data-breach-132-million/.

MITRE Partnership Network. "Group: Deep Panda, Shell Crew, …." *ATT&CK: Adversarial Tactics, Techniques, & Common Knowledge*. https://attack.mitre.org/wiki/Group/G0009.

MITRE Partnership Network. "Software: Sakula, Sakurel, VIPER." *ATT&CK: Adversarial Tactics, Techniques, & Common Knowledge*. https://attack.mitre.org/wiki/Software/S0074.

Murillo, Helen Klein. "A Summary of the Cybersecurity Executive Order." *Lawfare Institute*. May 11, 2017. https://www.lawfareblog.com/summary-cybersecurity-executive-order.

Nakashima, Ellen and Adam Goldman. "CIA pulled officers from Beijing after breach of federal personnel records." *The Washington Post*. September 29, 2015. https://www.washingtonpost.com/world/national-security/cia-pulled-officers-from-beijing-after-breach-of-federal-personnel-records/2015/09/29/1f78943c-66d1-11e5-9ef3-fde182507eac_story.html?noredirect=on&utm_term=.754b778d7a55.

Nakashima, Ellen and Adam Goldman. "U.S. intelligence head: CIA did not pull officers from Beijing after OPM hack." *The Washington Post*. November 2, 2015. https://www.washingtonpost.com/world/national-security/us-intelligence-head-cia-did-not-pull-officers-from-beijing-after-opm-hack/2015/11/02/8631aa4e-81a5-11e5-a7ca-6ab6ec20f839_story.html?utm_term=.153f8bca34d6.

Nakashima, Ellen. "Chinese government has arrested hackers it says breached OPM database." *The Washington Post*. December 2, 2015. 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?utm_term=.23171c02d1fc.

Nakashima, Ellen. "U.S. decides against publicly blaming China for data hack." *The Washington Post*. July 21, 2015. 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?utm_term=.a5aea01795eb.

Nakashima, Ellen. "With a series of major hacks, China builds a database on Americans." *The Washington Post*. June 5, 2015. https://www.washingtonpost.com/world/national-security/in-a-series-of-hacks-china-appears-to-building-a-database-on-americans/2015/06/05/d2af51fa-0ba3-11e5-95fd-d580f1c5d44e_story.html?utm_term=.f4927c010a3e.

Nash, Kim S. "Office of Personnel Management CIO to Leave in September." *The Wall Street Journal*. August 10, 2017. https://blogs.wsj.com/cio/2017/08/10/office-of-personnel-management-cio-to-leave-in-september/.

Newman, Lily Hay. "Taking Stock of Trump's Cybersecurity Executive Order So Far." *Wired*. September 3, 2017. https://www.wired.com/story/trump-cybersecurity-executive-order/.

Nextgov Staff. "48,000 Federal Employees Potentially Affected by Second Background Check Hack." *Nextgov*. December 18, 2014. http://www.nextgov.com/cybersecurity/2014/12/opm-alerts-feds-second-background-check-breach/101622/.

Noble, Zach. "Can America thump China for the OPM hack – and should it?" *FCW*. August 20, 2015. https://fcw.com/articles/2015/08/20/america-opm-hack.aspx.

Novetta and the Cyber Security Coalition. "Operation SMN: Axiom Threat Actor Group Report. 公理队." *Novetta*. October 27, 2014. http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf.

O'Connor, Nuala. "Why the OPM Data Breach is Unlike Any Other." *Center for Democracy & Technology*. June 22, 2015. https://cdt.org/blog/why-the-opm-data-breach-is-unlike-any-other/.

Ogrysko, Nicole. "OPM may have overestimated cost of ID theft services for cyber breach victims." *Federal News Radio*. March 31, 2017. https://federalnewsradio.com/opm-cyber-breach/2017/03/opm-may-overestimated-cost-id-theft-services-cyber-breach-victims/.

Perez, Evan and Shimon Prokupecz. "First on CNN: U.S. data hack may be 4 times larger than the government originally said." *CNN*. June 24, 2015. https://edition.cnn.com/2015/06/22/politics/opm-hack-18-milliion/index.html.

Perez, Evan. "FBI arrests Chinese national connected to malware used in OPM data breach." *CNN*. August 24, 2017. https://www.cnn.com/2017/08/24/politics/fbi-arrests-chinese-national-in-opm-data-breach/index.html.

Ragan, Steve. "FBI alert discloses malware tied to the OPM and Anthem attacks." *CSO*. June 30, 2015. https://www.csoonline.com/article/2942601/disaster-recovery/fbi-alert-discloses-malware-tied-to-the-opm-and-anthem-attacks.html.

Rohrlich, Justin. "How OPM Bilked a Security Contractor That Confirmed a Major Hack." *Foreign Policy*. September 7, 2016. http://foreignpolicy.com/2016/09/07/how-opm-bilked-a-security-contractor-that-confirmed-a-major-hack-cytech/.

Sanger, David E. "U.S. Decides to Retaliate Against China's Hacking." *The New York Times*. July 31, 2015. https://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html?_r=1.

Schmidt, Michael S., David E. Sanger, and Nicole Perlroth. "Chinese Hackers Pursue Key Data on U.S. Workers." *The New York Times.* July 9, 2014. https://www.nytimes.com/2014/07/10/world/asia/chinese-hackers-pursue-key-data-on-us-workers.html.

Segal, Adam. "The U.S.-China Cyber Espionage Deal One Year Later." *Council on Foreign Relations*. September 28, 2016. https://www.cfr.org/blog/us-china-cyber-espionage-deal-one-year-later.

Sevastopulo, Demetri and Geoff Dyer. "Obama and Xi in deal on cyber espionage." *Financial Times*. September 25, 2015. https://www.ft.com/content/0dbcab36-63be-11e5-a28b-50226830d644.

Shalal, Andrea and Matt Spetalnick. "Data hacked from U.S. government dates back to 1985: U.S. official." *Reuters*. June 5, 2015. https://www.reuters.com/article/us-cybersecurity-usa/data-hacked-from-u-s-government-dates-back-to-1985-u-s-official-idUSKBN0OL1V320150606?irpc=932.

Shear, Michael D. and Scott Shane. "White House Weighs Sanctions After Second Breach of a Computer System." *The New York Times.* June 12, 2015. https://www.nytimes.com/2015/06/13/us/white-house-weighs-sanctions-after-second-breach-of-a-computer-system.html?_r=0.

Singer, Peter Warren. "Life After the OPM Hack." *New America.* December 12, 2016. https://www.newamerica.org/cybersecurity-initiative/podcasts/life-after-opm-attack/.

Starks, Tim. "OPM spared lawsuits over massive breach." *Politico.* September 20, 2017. https://www.politico.com/tipsheets/morning-cybersecurity/2017/09/20/opm-spared-lawsuits-over-massive-breach-222379.

Sternstein, Aliya and Jack Moore. "Timeline: What We Know About the OPM Breach (UPDATED)." *Nextgov.* June 26, 2015. http://www.nextgov.com/cybersecurity/2015/06/timeline-what-we-know-about-opm-breach/115603/.

Strohm, Chris. "Hacked OPM Data Hasn't Been Shared or Sold, Top Spy-Catcher Says." *Bloomberg*. September 28, 2017. https://www.bloomberg.com/news/articles/2017-09-28/hacked-opm-data-hasn-t-been-shared-or-sold-top-spy-catcher-says.

The White House. Office of the Press Secretary. "FACT SHEET: Administration Cybersecurity Efforts 2015." *The White House*. July 09, 2015. https://obamawhitehouse.archives.gov/the-press-office/2015/07/09/fact-sheet-administration-cybersecurity-efforts-2015.

The White House. Office of the Press Secretary. "FACT SHEET: Cybersecurity National Action Plan." *The White House*. February 9, 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

The White House. Office of the Press Secretary. "FACT SHEET: President Xi Jinping's State Visit to the United States." *The White House*. September 25, 2015. https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

Thornton, David. "Judge dismisses OPM data breach lawsuits, union appeals." *Federal News Radio.* September 21, 2017. https://federalnewsradio.com/opm-cyber-breach/2017/09/judge-dismisses-opm-cyber-breach-lawsuits-union-appeals/.

Townsend, Chris. "OPM Breach Costs Could Exceed $1 Billion." *Symantec Official Blog*. March 23, 2017. https://www.symantec.com/connect/blogs/opm-breach-costs-could-exceed-1-billion.

U.S. Congress. House. Committee on Oversight and Government Reform. *Memorandum: Committee Investigation into the OPM Data Breach*. 114th Cong., September 6, 2016. https://democrats-oversight.house.gov/sites/democrats.oversight.house.gov/files/documents/2016-09-06.Democratic%20Memo%20on%20OPM%20Data%20Breach%20Investigation.pdf.

U.S. Congress. House. Committee on Oversight and Government Reform. *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation.* 114th Cong., September 7, 2016. https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf.

U.S. Congress. House. Committee on Oversight and Government Reform. Subcommittee on Information Technology. *Cybersecurity: The Department of the Interior*. 114th Cong., 1st sess., July 15, 2015. https://oversight.house.gov/wp-content/uploads/2016/04/7-15-15-Cybersecurity-The-Department-of-the-Interior.pdf.

U.S. Department of Commerce. National Institute of Standards and Technology. Information Technology Laboratory. Applied Cybersecurity Division. Trusted Identities Group. "Back to basics: Multi-factor authentication (MFA)." https://www.nist.gov/itl/tig/back-basics-multi-factor-authentication.

U.S. Department of Homeland Security. "Cybersecurity." https://www.dhs.gov/topic/cybersecurity.

U.S. Department of Homeland Security. Office of Inspector General. *Management Advisory Report: A Guide for Assessing Cybersecurity within the Office of Inspector General Community.* OIG-14-43. February 2014.

https://www.ignet.gov/sites/default/files/files/Cybersecurity%20Assessment%20-%20Feb%202014.pdf.

U.S. Department of Homeland Security. United States Computer Emergency Readiness Team. "About Us." *US-CERT.* https://www.us-cert.gov/about-us.

U.S. Department of Homeland Security. United States Computer Emergency Readiness Team. "Information Sheet: US-CERT." *US-CERT*. https://www.us-cert.gov/sites/default/files/publications/infosheet_US-CERT_v2.pdf.

U.S. Department of Homeland Security. United States Computer Emergency Readiness Team. "October is National Cybersecurity Awareness Month." *US-CERT*. October 2, 2017. https://www.us-cert.gov/ncas/current-activity/2017/10/01/October-National-Cybersecurity-Awareness-Month.

U.S. Department of Justice. Federal Bureau of Investigation. "FBI Investigating OPM Cyber Intrusion." *FBI.gov*. June 4, 2015. https://www.fbi.gov/news/stories/fbi-investigating-opm-cyber-intrusion.

U.S. Department of Justice. Federal Bureau of Investigation. Cyber Division. "FBI FLASH: Alert Number A-000061-MW." June 5, 2015. https://info.publicintelligence.net/FBI-HackToolsOPM.pdf.

U.S. Government Accountability Office. *Information Security: OPM Has Improved Controls, but Further Efforts are Needed*. GAO-17-614. Washington, D.C., August 2017. https://www.gao.gov/assets/690/686400.pdf.

U.S. Library of Congress. Congressional Research Service. *Cyber Intrusion into U.S. Office of Personnel Management: In Brief*, by Kristin Finklea, Michelle D. Christensen, Eric A. Fischer, Susan V. Lawrence, and Catherine A. Theohary. R44111. July 17, 2015. https://fas.org/sgp/crs/natsec/R44111.pdf.

U.S. Library of Congress. Congressional Research Service. *Cybersecurity Issues and Challenges: In Brief*, by Eric A. Fischer. R43831. August 12, 2016. https://fas.org/sgp/crs/misc/R43831.pdf.

U.S. Library of Congress. Congressional Research Service. *OPM Data Breach: Personnel Security Background Investigation Data,* by Michelle D. Christensen. IN10327. July 24, 2015. https://fas.org/sgp/crs/natsec/IN10327.pdf.

U.S. Library of Congress. Congressional Research Service. *U.S.-China Cyber Agreement*, by John W. Rollins. IN10376. October 16, 2015. https://fas.org/sgp/crs/row/IN10376.pdf.

U.S. Office of Management and Budget. Deputy Director for Management. *Memorandum for the Heads of Executive Departments and Agencies: Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, by Clay Johnson III. M-07-16. May 22, 2007.

U.S. Office of Personnel Management, Cybersecurity Resource Center. "Cybersecurity Incidents." OPM.GOV. https://www.opm.gov/cybersecurity/cybersecurity-incidents/.

U.S. Office of Personnel Management. "About Us." *OPM.gov*. https://www.opm.gov/about-us/.

U.S. Office of Personnel Management. "Actions to Strengthen Cybersecurity and Protect Critical IT Systems." June 2015. https://www.opm.gov/cybersecurity/cybersecurity-incidents/opm-cybersecurity-action-report.pdf.

U.S. Office of Personnel Management. "Annual Performance Report: Fiscal Year 2017." *OPM.gov*. February 2018. https://www.opm.gov/about-us/budget-performance/performance/2017-annual-performance-report.pdf.

U.S. Office of Personnel Management. "Cybersecurity Resource Center." *OPM.gov*. https://www.opm.gov/cybersecurity/.

U.S. Office of Personnel Management. "OPM to Notify Employees of Cybersecurity Incident." *OPM.gov*. June 4, 2015. https://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident/.

U.S. Office of Personnel Management. "Our Inspector General." *OPM.gov*. https://www.opm.gov/about-us/our-inspector-general/.

U.S. Office of Personnel Management. "Our Mission, Role & History." *OPM.gov*. https://www.opm.gov/about-us/our-mission-role-history/agency-leadership/.

U.S. Office of Personnel Management. "Our People & Organization: Senior Staff Bios." *OPM.gov*. https://www.opm.gov/about-us/our-people-organization/senior-staff-bios/.

U.S. Office of Personnel Management. "Our People & Organization: Senior Staff Bios." *OPM.gov*. https://www.opm.gov/about-us/our-people-organization/senior-staff-bios/.

U.S. Office of Personnel Management. "Questionnaire for National Security Positions." Standard Form 86. OMB No. 3206 0005. *OPM.gov.* Revised December 2010. https://www.opm.gov/forms/pdf_fill/sf86-non508.pdf.

U.S. Office of Personnel Management. "Standard Forms." *OPM.gov*. https://www.opm.gov/forms/standard-forms/.

U.S. Office of Personnel Management. "What We Do." *OPM.gov*. https://www.opm.gov/about-us/our-mission-role-history/what-we-do/.

U.S. Office of Personnel Management. Office of Communications. "OPM Announces Steps to Protect Federal Workers and Others from Cyber Threats." *OPM.gov*. June 9, 2015. https://www.opm.gov/news/releases/2015/07/opm-announces-steps-to-protect-federal-workers-and-others-from-cyber-threats/.

U.S. Office of Personnel Management. Office of Communications. "OPM welcomes Dr. Jeff T.H. Pon as 11th director of the agency." *OPM.gov*. March 12, 2018. https://www.opm.gov/news/releases/2018/03/opm-welcomes-dr-jeff-t-h-pon-as-11th-director-of-the-agency/.

U.S. Office of Personnel Management. Office of Communications. "Statement: OPM names new Chief Information Officer." *OPM.gov*. October 2, 2017. https://www.opm.gov/news/releases/2017/10/statement-opm-names-new-chief-information-officer/.

U.S. Office of Personnel Management. Office of the Inspector General. Office of Audits. "Federal Information Security Management Act Audit FY 2007." 4A-CI-00-07-007. September 18, 2007.

U.S. Office of Personnel Management. Office of the Inspector General. Office of Audits. "FY 2007 Federal Information Security Management Act Follow-Up Audit." 4A-CI-00-07-008. September 18, 2007.

U.S. Office of Personnel Management. Office of the Inspector General. Office of Audits. "FY 2008 Federal Information Security Management Act Follow-Up Audit." 4A-CI-00-08-061. September 16, 2008.

U.S. Office of Personnel Management. Office of the Inspector General. Office of Audits. "Federal Information Security Management Act Audit FY 2008." 4A-CI-00-08-022. September 23, 2008.

U.S. Office of Personnel Management. Office of the Inspector General. Office of Audits. "Federal Information Security Management Act Audit FY 2009." 4A-CI-00-09-031. November 5, 2009.

U.S. Office of Personnel Management. Office of the Inspector General. Office of Audits. "Federal Information Security Management Act Audit FY 2010." 4A-CI-00-10-019. November 10, 2010.

U.S. Office of Personnel Management. Office of the Inspector General. Office of Audits. "Federal Information Security Management Act Audit FY 2011." 4A-CI-00-11-009. November 9, 2011.

U.S. Office of Personnel Management. Office of the Inspector General. Office of Audits. "Federal Information Security Management Act Audit FY 2012." 4A-CI-00-12-016. November 5, 2012.

U.S. Office of Personnel Management. Office of the Inspector General. Office of Audits. "Federal Information Security Management Act Audit FY 2013." 4A-CI-00-13-021. November 21, 2013.

U.S. Office of Personnel Management. Office of the Inspector General. Office of Audits. "Federal Information Security Management Act Audit FY 2014." 4A-CI-00-14-016. November 12, 2014.

U.S. Office of Personnel Management. Office of the Inspector General. Office of Audits. "Federal Information Security Modernization Act Audit FY 2015." 4A-CI-00-15-011. November 10, 2015.

U.S. Office of Personnel Management. Office of the Inspector General. Office of Audits. "Federal Information Security Modernization Act Audit Fiscal Year 2016." 4A-CI-00-16-039. November 9, 2016.

U.S. Office of Personnel Management. Office of the Inspector General. Office of Audits. "Federal Information Security Modernization Act Audit Fiscal Year 2017." 4A-CI-00-17-020. October 27, 2017.

U.S. Office of Personnel Management. Office of the Inspector General. "Open Recommendations Over Six Months Old as of September 30, 2017." December 1, 2017. https://www.opm.gov/our-inspector-general/open-recommendations/open-recommendations-over-six-months-old-as-of-september-30-2017.pdf.

U.S. Office of the Director of National Intelligence. "2014 Report on Security Clearance Determinations." *DNI.gov*. April 2015. https://www.dni.gov/files/documents/2015-4-21%20Annual%20Report%20on%20Security%20Clearance%20Determinations.pdf.

United States of America v. YU PINGAN, a.k.a. "GoldSun." 17 MJ 2970. (Cal.2017).

Viswanatha, Aruna and Robert McMillan. "Chinese National Charged with Providing Hackers With Malware Linked to OPM Breach." *The Wall Street Journal*. August 24, 2017. https://www.wsj.com/articles/chinese-national-charged-with-providing-hackers-with-malware-linked-to-opm-breach-1503626027

Wagner, Erich. "OPM Gets a Permanent Director After Nearly 3 Years of Acting Leaders." *Government Executive*. March 8, 2018. https://www.govexec.com/management/2018/03/senate-confirms-opm-director/146499/.

Wittes, Benjamin. "Whose Fault is the OPM Hack Really?" *Lawfare Institute*. June 25, 2015. https://www.lawfareblog.com/whose-fault-opm-hack-really.

Wittes, Benjamin. "Whose Fault is the OPM Hack, Really? Part II." *Lawfare Institute*. June 30, 2015. https://www.lawfareblog.com/whose-fault-opm-hack-really-part-ii.

Zetter, Kim and Andy Greenberg. "Why the OPM Breach is Such a Security and Privacy Debacle." *Wired*. June 11, 2015. https://www.wired.com/2015/06/opm-breach-security-privacy-debacle/.

Civil Service Reform Act of 1978, 5 U.S. Code 1101. Public Law 95-454, 92 Stat. 1119-1227. October 13, 1978. https://www.gpo.gov/fdsys/pkg/STATUTE-92/pdf/STATUTE-92-Pg1111.pdf.

"Once more, a breach." *The Economist*. June 5, 2015. https://www.economist.com/news/china/21653722-massive-cyber-intrusion-may-prove-be-latest-glitch-us-china-relations-hacked.

"OPM Breach Analysis: Update." *ThreatConnect*. June 9, 2015. https://www.threatconnect.com/blog/opm-breach-analysis-update/.

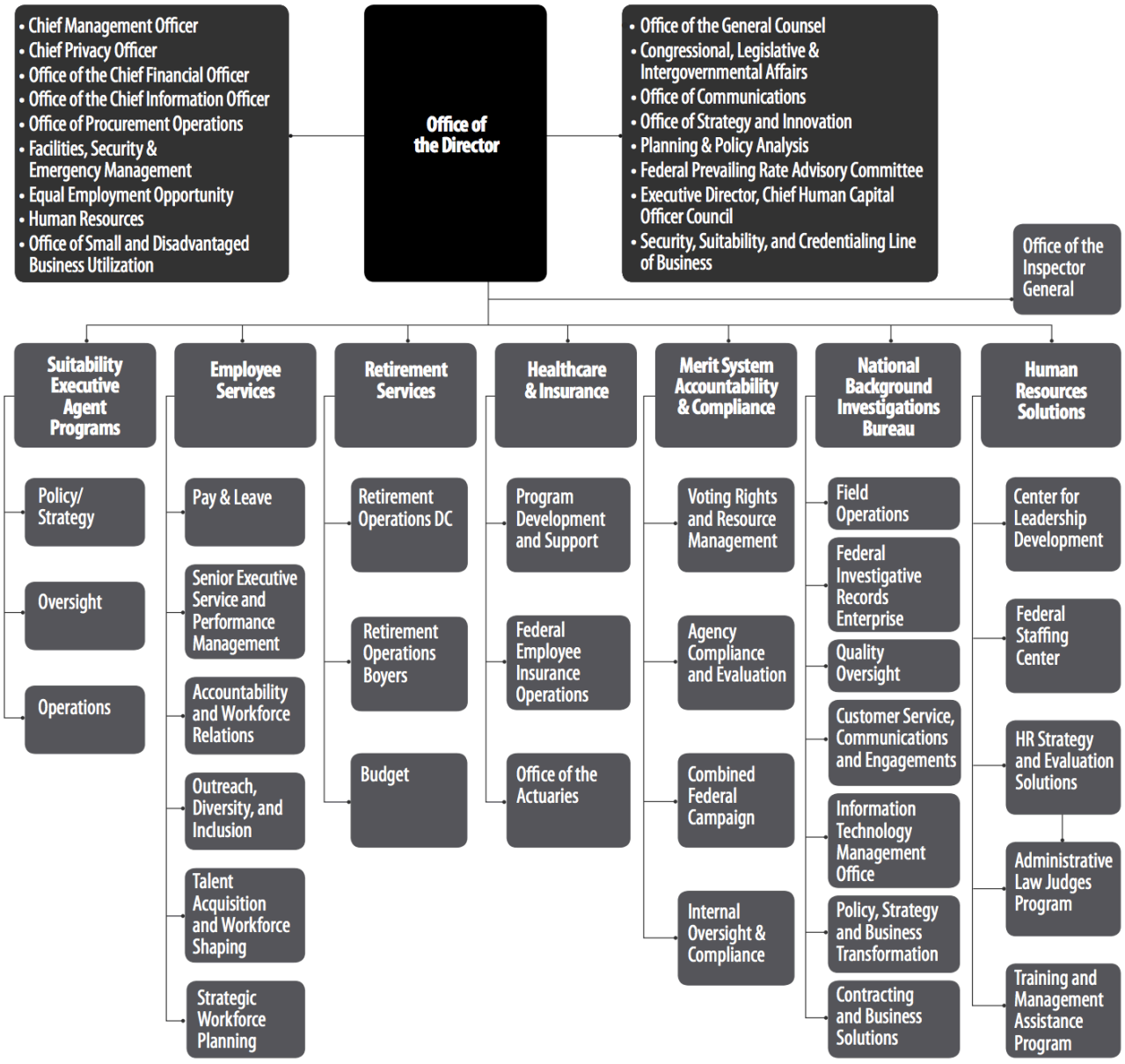
Executive Order No. 13800. 3 C.F.R. 22391 (May 11, 2017). https://www.gpo.gov/fdsys/pkg/FR-2017-05-16/pdf/2017-10004.pdf.

Peterson, Andrea. "OPM says 5.6 million fingerprints stolen in cyberattack, five times as many as previously thought." *The Washington Post*. September 23, 2015. https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/?utm_term=.7cdc1f94edd5.

Eng, James. "OPM Hack: Government Finally Starts Notifying 21.5 Million Victims. "*NBC News*. October 1, 2015. https://www.nbcnews.com/tech/security/opm-hack-government-finally-starts-notifying-21-5-million-victims-n437126.

Auerbach, David. "The OPM Breach Is a Catastrophe." *Slate*. June 16, 2015. http://www.slate.com/articles/technology/future_tense/2015/06/opm_hack_it_s_a_catastrophe_here_s_how_the_government_can_stop_the_next.html.

Appendix I: OPM Organizational Chart



Source: U.S. Office of Personnel Management, "Annual Performance Report: Fiscal Year 2017," *OPM.gov*, February 2018, https://www.opm.gov/about-us/budget-performance/performance/2017-annual-performance-report.pdf, 1

Appendix II: Historical Dataset of OPM OIG FISMA Recommendations

	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	TOTAL	AVG LIFE (YEARS)
Total Recommendations	9	19	34	41	29	18	16	29	27	26	39	287	2.7871032
New Recommendations	9	17	24	16	23	10	4	19	6	9	18	155	1.6673442
Rollover Recommendations	0	2	10	25	6	8	12	10	21	17	21	132	
Year Closed	0	6	8	9	37	21	8	6	10	6	5	116	1.5228389
Closed (Orig Year)	9	16	24	16	22	8	3	9	5	4	0	116	1.5228389
% Closed (Orig Year)	100%	84%	71%	39%	76%	44%	19%	31%	19%	15%	0%		
Closed (By Year Closed)	0	6	8	9	37	21	8	6	10	6	5	116	
% Closed (of total closed, by year closed)	0%	5%	7%	8%	32%	18%	7%	5%	9%	5%	4%		
Open	0	1	0	0	1	2	1	10	1	5	18	39	2.0971549
Total Recs YoY	0%	111%	79%	21%	-29%	-38%	-11%	81%	-7%	-4%	50%	8%	
New Recs YoY	0%	89%	41%	-33%	44%	-57%	-60%	375%	-68%	50%	100%	1%	
Rollover Recs YoY	0%	0%	400%	150%	-76%	33%	50%	-17%	110%	-19%	24%	30%	
Closed Recs YoY	0%	0%	33%	13%	311%	-43%	-62%	-25%	67%	-40%	-17%	-2%	

CATEGORIES - ALL	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	TOTAL	AVG LIFE (YEARS)	% RECS
Agency Privacy Program	2	1	7	4	4	1	1	0	0	0	0	20	3.7667123	7%
Configuration Management	1	4	8	10	5	3	3	8	7	8	11	68	2.6260677	24%
Contingency Planning	1	0	3	3	3	2	2	3	2	2	3	24	3.3312785	8%
Identity, Credential, and Access Management	1	1	2	5	7	4	2	3	5	4	5	39	2.1364946	14%
Incident Response Program	2	3	0	0	0	1	1	2	1	1	0	11	1.9947696	4%
Information Security Continuous Monitoring	0	1	0	2	2	2	2	2	2	2	3	18	2.008067	6%
Information Security Governance	2	1	5	2	2	1	2	2	2	3	1	23	4.0958904	8%
Risk Management	0	5	5	6	3	3	3	6	4	2	12	49	2.6886777	17%
Security Assessment and Authorization	0	2	4	7	2	0	0	3	3	3	2	26	3.0807165	9%
Security Training	0	1	0	2	1	1	0	0	1	1	2	9	2.0645358	3%
TOTAL	9	19	34	41	29	18	16	29	27	26	39	287	2.7871032	

CATEGORIES - ALL UNIQUE	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	TOTAL	AVG LIFE (YEARS)	% RECS
Agency Privacy Program	2	1	5	0	3	0	0	0	0	0	0	11	1.837609	7%
Configuration Management	1	4	6	3	4	2	2	6	1	1	4	34	1.7693795	22%
Contingency Planning	1	0	2	0	3	1	0	1	0	0	1	9	2.235312	6%
Identity, Credential, and Access Management	1	1	2	4	5	3	0	1	1	1	3	22	1.2603985	14%
Incident Response Program	2	2	0	0	0	1	0	2	1	1	0	9	0.8961948	6%
Information Security Continuous Monitoring	0	1	0	2	2	1	1	1	1	1	2	12	1.5678082	8%
Information Security Governance	2	0	4	1	1	0	0	1	0	2	0	11	2.3312578	7%
Risk Management	0	5	3	1	3	2	1	4	1	2	6	28	1.7618395	18%
Security Assessment and Authorization	0	2	2	3	2	0	0	3	0	0	0	12	1.7979452	8%
Security Training	0	1	0	2	0	0	0	0	1	1	2	7	0.969863	5%
TOTAL	9	17	24	16	23	10	4	19	6	9	18	155		

CATEGORIES - ROLLOVER	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	TOTAL	AVG LIFE (YEARS)	% RECS
Agency Privacy Program	0	0	2	4	1	1	1	0	0	0	0	9	8.3704718	7%
Configuration Management	0	0	2	7	1	1	1	2	6	7	7	34	5.2521354	26%
Contingency Planning	0	0	1	3	0	1	2	2	2	2	2	15	5.3300457	11%
Identity, Credential, and Access Management	0	0	0	1	2	1	2	2	4	3	2	17	4.9013699	13%
Incident Response Program	0	1	0	0	0	0	1	0	0	0	0	2	10.971233	2%
Information Security Continuous Monitoring	0	0	0	0	0	1	1	1	1	1	1	6	6.0242009	5%
Information Security Governance	0	1	1	1	1	1	2	1	2	1	1	12	7.8504566	9%
Risk Management	0	0	2	5	0	1	2	2	3	0	6	21	6.2735812	16%
Security Assessment and Authorization	0	0	2	4	0	0	0	0	3	3	2	14	5.7213307	11%
Security Training	0	0	0	0	1	1	0	0	0	0	0	2	9.290411	2%
TOTAL	0	2	10	25	6	8	12	10	21	17	21	132	6.0598381	

UNIQUE CATEGORIES - BY YEAR OPEN	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	TOTAL	AVG LIFE (YEARS)	% RECS
Agency Privacy Program	2	1	5	0	3	0	0	0	0	0	0	11	1.837609	9%
Configuration Management	1	4	6	3	4	2	2	1	0	0	0	23	1.64324	20%
Contingency Planning	1	0	2	0	3	0	0	0	0	0	0	6	1.8191781	5%
Identity, Credential, and Access Management	1	1	2	4	5	2	0	1	1	0	0	17	1.1574537	15%
Incident Response Program	2	2	0	0	0	1	0	2	1	1	0	9	0.8961948	8%
Information Security Continuous Monitoring	0	0	0	2	2	1	1	1	1	1	0	9	0.9388128	8%
Information Security Governance	2	0	4	1	1	0	0	1	0	1	0	10	2.4257534	9%
Risk Management	0	5	3	1	2	2	0	2	1	0	0	16	1.657363	14%
Security Assessment and Authorization	0	2	2	3	2	0	0	1	0	0	0	10	1.4813699	9%
Security Training	0	1	0	2	0	0	0	0	1	1	0	5	1.1890411	4%
TOTAL	9	16	24	16	22	8	3	9	5	4	0	116		

UNIQUE CATEGORIES - BY YEAR CLOSED	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	TOTAL	AVG LIFE (YEARS)	% RECS
Agency Privacy Program	0	1	0	4	2	3	0	1	0	0	0	11	1.837609	9%
Configuration Management	0	1	1	1	10	4	2	2	1	1	0	23	1.64324	20%
Contingency Planning	0	1	0	0	2	2	0	0	1	0	0	6	1.8191781	5%
Identity, Credential, and Access Management	0	1	1	1	4	5	2	1	1	1	0	17	1.1574537	15%
Incident Response Program	0	2	2	0	0	0	1	0	3	0	1	9	0.8961948	8%
Information Security Continuous Monitoring	0	0	0	0	2	2	1	1	1	1	1	9	0.9388128	8%
Information Security Governance	0	0	0	2	4	1	0	0	1	1	1	10	2.4257534	9%
Risk Management	0	0	2	0	7	2	1	1	1	2	0	16	1.657363	14%
Security Assessment and Authorization	0	0	1	1	5	2	0	0	0	0	1	10	1.4813699	9%
Security Training	0	0	1	0	1	0	1	0	1	0	1	5	1.1890411	4%
TOTAL	0	6	8	9	37	21	8	6	10	6	5	116		

UNIQUE CATEGORIES - OPEN	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	TOTAL	AVG LIFE (YEARS)	% RECS
Agency Privacy Program	0	0	0	0	0	0	0	0	0	0	0	0	0	0%
Configuration Management	0	0	0	0	0	0	0	5	1	1	4	11	2.0331258	28%
Contingency Planning	0	0	0	0	0	1	0	1	0	0	1	3	3.0675799	8%
Identity, Credential, and Access Management	0	0	0	0	0	1	0	0	0	1	3	5	1.610411	13%
Incident Response Program	0	0	0	0	0	0	0	0	0	0	0	0	0	0%
Information Security Continuous Monitoring	0	1	0	0	0	0	0	0	0	0	2	3	3.4547945	8%
Information Security Governance	0	0	0	0	0	0	0	0	0	1	0	1	1.3863014	3%
Risk Management	0	0	0	0	1	0	1	2	0	2	6	12	1.9011416	31%
Security Assessment and Authorization	0	0	0	0	0	0	0	2	0	0	0	2	3.3808219	5%
Security Training	0	0	0	0	0	0	0	0	0	0	2	2	0.4219178	5%
TOTAL	0	1	0	0	1	2	1	10	1	5	18	39		

Appendix III: Recommendations for OPM

Recommendation 1: *Prioritize Implementation of Oldest Open OIG FISMA Recommendations*

The **Director of OPM** and the **Office of the Chief Information Officer** should work with **all relevant program offices** to prioritize the necessary resources, time, and personnel to implement all Inspector General FISMA audit recommendations that have been **open for two years or more** before the issuance of the OIG's FY 2018 FISMA audit. Prioritizing these 16 open recommendations (as of March 30, 2018) would improve historically problematic recommendation categories for OPM, such as information security continuous monitoring; risk management; and identity, credential, and access management.

Recommendation 2: *Develop Security Best Practices through Continuous Improvement*

The **Director of OPM** and the **Office of the Chief Information Officer** should draft and publish a draft strategy document developing a set of best practices focused on best-demonstrated continuous-improvement processes as documented in the latest revision of the *NIST Framework for Improving Critical Infrastructure Cybersecurity*, including the key functions of **identification** of; **protection** from; **detection** of; **response** to; and **recovery** from cyber espionage, cyber breaches, cyberattack, and other malicious cyber activities, **by the end of FY 2018.**

Recommendation 3: *Evolve the Contractor Relationship*

The **Director of OPM** and **all related program offices** should act to facilitate an evolution in the contractor relationship to better manage the risks associated with contractors providing key services for the agency. These actions should include, as a baseline, improved identity verification; consolidated credential management; and more granular access management. These new policies should be published **by the end of FY 2018** and enacted either **by the end of FY 2018** or the next OPM contractor services agreement following policy publication, **whichever is sooner.**

Recommendation 4: *Restructure IT Security Training Programs*

The **Director of OPM** and the **Office of the Chief Information Officer**, working with **all relevant OPM program offices,** should publish findings on all agency security training efforts, including all cybersecurity-related education curricula, training percentage rates, and training retention; report these findings to the OIG in a timely manner; and develop and restructure IT security training programs accordingly to maximize training effectiveness and concept retention among all OPM employees and contractors.

Recommendation 5: *Develop Public-Private Partnerships for Information Sharing*

The Director of OPM, in a cross-agency effort with all other executive branch offices and FISMA-designated cybersecurity response agencies, should author and publish a report on public-private partnerships for cybersecurity information sharing and incident response within 180 days and develop an actionable timeline for working with the private sector entities identified in the report within 180 days of the report's release.

About the Author

Zeyi Lin was born in Nanjing, China on June 14, 1995, and moved with his family to Austin, Texas in 2001. He enrolled in the Plan II Honors program at the University of Texas at Austin in 2013 and concurrently studied Electrical and Computer Engineering and Government. In college, he was actively involved with the Society of Plan II Engineers and the Texas Blazers, a service, spirit, and leadership organization. He was selected as a University of Texas System Archer Fellow and interned in the Obama-era White House Office of Science and Technology Policy in the fall of 2015. He graduated Phi Beta Kappa and as a College of Liberal Arts Dean's Distinguished Graduate in May 2018. Mr. Lin will intern with the Institute of Electrical and Electronics Engineers as a Technology Policy Analyst in Washington, D.C., this summer and plans to join Bain & Company as an Associate Consultant this fall.