Catholic University Journal of Law and Technology

Volume 24 | Issue 2 Article 7

2016

Time to Rethink Cybersecurity Reform: The OPM Data Breach and the Case for Centralized Cybersecurity Infrastructure

Zachary Figueroa
Catholic University of America, Columbus School of Law

TIME TO RETHINK CYBERSECURITY REFORM: THE OPM DATA BREACH AND THE CASE FOR CENTRALIZED CYBERSECURITY INFRASTRUCTURE

Zachary Figueroa*

INTRODUCTION

Cybersecurity breaches remain a clear and pervasive risk to the privacy of one's personal data and information. As of July 2015, 888 cybersecurity breaches were reported involving some-245.9 million records compromised worldwide for just that single year.[1] Given the increasing severity and complexity of cyber threats and incidents, this reality logically raises the poignant issue of whether the breach of U.S. Office of Personnel Management ("OPM") is a different type of breach or—for that matter—a big deal?[2] The answer is a resounding "yes." The magnitude and depth of this breach of the Federal Government, must immediately call into question the United States' cybersecurity policies and the troubling track record of various federal agencies ability to

* J.D. Candidate, The Catholic University of America - Columbus School of Law, 2016; M.S. Business Analytics, The Catholic University of America, 2015; B.A. Political Science, Biola University, 2013; B.S. Business Administration - Marketing, Biola University, 2012. I gratefully thank Ned Steiner and Michelle Curth for their thoughtful comments and editorial savvy throughout my entire writing process, Richard Kisielowski and the entire staff of THE CATHOLIC UNIVERSITY JOURNAL OF LAW & TECHNOLOGY, Volume 24, for their patience and commitment in the development of this Comment, and furthermore my family and friends who have graciously supported and encouraged me not only in the research and writing of this Comment but in all my endeavors.

1 GEMALTO, INDEX 2015 FIRST HALF REVIEW: FINDINGS FROM THE BREACH LEVEL INDEX 3 (2015), http://bit.ly/244WHpj ("[D]ata records stolen from state-sponsored attacks rose dramatically compared to previous years and healthcare and government over took retail as the major sectors under siege with the number of compromised data records.").

2 *Id.* at 3 ("The biggest breach in the first half of this year, which scored a 10 on the Breach Level Index magnitude scale, was an identity theft attack on Anthem Insurance that exposed 78.8 million records…the analysis period included a breach of 21 million records at [OPM] with a Breach Level Index of 9.7…."); *see also* IDENTITY THEFT RESOURCE CTR., DATA BREACH REPORTS 20, 120 (2015), http://bit.ly/1XOPp6W.

properly secure sensitive state information and citizens' private data.[3] While most private sector breaches are dealt with relatively quickly to ensure consumer confidence,[4] the Federal Government lacks this agility to spring to action.

Unable to blame on any one person for this security failure, politicians continue to decry the OPM Breach as a categorical failure of the Federal Government.[5] Some suggest this incident is the most detrimental breach of national security since the terrorist attacks of September 11th,[6] and have dubbed it a "Cyber Pearl Harbor."[7] While not all critics have gone so far as to make such a dramatic correlation, many agree the failure to protect OPM's systems is a "data rupture,"[8] or "mega breach"[9]—one of the largest in United States history to date.[10] Regardless of the moniker, the effects of the OPM Breach and theft of personal data on millions of Americans are serious and will result long-lasting

---

3 *See*, *e.g.*, SEN. TOM COBURN, THE FEDERAL GOVERNMENT'S TRACK RECORD ON CYBERSECURITY AND CRITICAL INFRASTRUCTURE 2-3 (2014), http://1.usa.gov/1Mn4090 (highlighting "real lapses by the federal government" with regard to significant breaches in cybersecurity); *see also* S. REP. NO. 113-240 2 (2014) ("The United States has also seen widespread targeting of, theft, and disruption of information stored on the federal government's own networks, where sensitive information, including information related to the operations of critical infrastructure, is at risk of disclosure.").

4 *See*, *e.g.*, Eric Dezenhall, *A Look Back at the Target Breach*, HUFF. POST (April 6, 2015, 10:30 AM), http://huff.to/1T72zND (explaining that more than 100 million people were reportedly affected by the Target breach and in the wake of stockholder backlash the company spent nearly $252 million to combat the breach, including an additional $10 million for customers who could reasonably prove their account was severely compromised because of the breach).

5 Press Release, House Comm. on Oversight and Gov. Reform, Chaffetz Statement on Latest OPM Data Breach Revelation (July 9, 2015), http://1.usa.gov/244WHG2 ("[S]uch incompetence is inexcusable.…"); *see also* Ellen Nakashima, *Chinese breach data of 4 million federal workers*, WASH. POST (June 4, 2015), http://wapo.st/22x7bT8 [hereinafter Nakashima I] (statement of California Rep. Adam Schiff).

> This latest intrusion…is among the most shocking because Americans may expect that federal computer networks are maintained with state-of-the-art defenses, the cyberthreat from hackers, criminals, terrorists and state actors is one of the greatest challenges we face on a daily basis, and it's clear that a substantial improvement in our cyber databases and defenses is perilously overdue.

Id.

6 Steve Weisman, *The hacking of OPM: Is it our cyber 9/11?*, USA TODAY (June 13, 2015, 9:04 AM), http://usat.ly/1UNLrMF.

7 Noah Rothman, *The Cyber Pearl Harbor and the Inescapable Gravity of Geopolitics*, COMMENTARY MAG. (June 5, 2015), http://bit.ly/1VHmmUi.

8 Dan Goodin, *Call it a "data rupture": Hack hitting OPM affects 21.5 million*, ARS TECHNICA (July 9, 2015, 6:10 PM), http://bit.ly/22x7nBV.

9 John Eggerton, *OPM Director Resigns in Wake of Mega-Breach*, MULTICHANNEL (July 10, 2015, 1:15 PM), http://bit.ly/1Mn4oEo.

10 Ellen Nakashima, *Hacks of OPM databases compromised 22.1 million people, federal authorities say*, WASH. POST (July 9, 2015), http://wapo.st/21I9gWp.

implications for how the nation must manage and protect sensitive data going forward.

The Obama Administration touted progress when it promotes cybersecurity legislation that imposes liability against the private sector as an effort to mitigate data breaches.[11] However, the OPM Breach highlights the Federal Government's flawed and misguided understanding of cybersecurity. The current framework aggressively penalizes the private sector when it fails to secure individual's data, yet falters when policing its own internal policies and agency actions.[12] Congressman Will Hurd [R-TX] recently noted, "[t]he hypocrisy is that while the government leaves its networks and the data of millions of Americans at risk, it fines private companies for security breaches."[13] In the aftermath of the OPM Breach, the time to reevaluate the nation's cybersecurity strategy and the ability of the Federal Government to secure itself, its employees, its agencies, and ultimately the American people is now.

The Federal Government must develop a system that more effectively allocates resources and cybersecurity expertise at home. The backbone of any federal cybersecurity policy that promotes national security and economic prosperity must include a bilateral, international dialogue against state-sponsored cyber espionage, whether directed toward the government or the private sector.[14] The OPM Breach highlights the ineffective, fragmented approach the

---

[11] Press Release, The White House, Office of the Press Secretary, FACT SHEET: Administration Cybersecurity Efforts 2015 (July 9, 2015), http://1.usa.gov/1pJlHWy [*hereinafter* White House - Administration Cybersecurity Efforts 2015].

> From the beginning of his Administration, the President has made it clear that cybersecurity is one of the most important challenges we face as a Nation. In response, the U.S. Government has implemented a wide range of policies, both domestic and international, to improve our cyber defenses, enhance our response capabilities, and upgrade our incident management tools.

Id.

[12] FED. TRADE COMMISSION., 2014 PRIVACY AND DATA SECURITY UPDATE 5 (2014), http://1.usa.gov/1pJm2IV ("Since 2002, the FTC has brought over 50 cases against companies that have engaged in unfair or deceptive practices that put consumers' personal data at unreasonable risk."); Press Release, U.S. Dep't of Health & Human Serv., Data breach results in $4.8 million HIPAA settlements (May 7, 2014), http://1.usa.gov/1RyWq7e (stating HHS had reached a resolution agreement with New York and Presbyterian Hospital to pay the Office of Civil Rights $3,300,000 to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 Privacy and Security Rules as well as Columbia University to pay $1,500,000).

[13] Will Hurd, *Cleaning Up the Federal Cyber Debacle*, WALL ST. J. (June 25, 2015, 7:09 PM), http://on.wsj.com/1SiCJDV.

[14] KRISTEN FINKLEA, ET AL., CONG. RESEARCH SERV., R44111, CYBER INTRUSION INTO U.S. OFFICE OF PERSONNEL MANAGEMENT: IN BRIEF 2-3 (2015), http://bit.ly/1Psy8KJ ("Determining an actor (and actor's motivation) involved in a cyber incident can help guide how the United States responds…If the perpetrator is deemed to be a state-sponsored actor with a different motivation, the United States may utilize diplomatic or military tools in its response.").

Federal Government has previously utilized in modernizing federal cybersecurity. There is a pressing need for the United States Congress to enact legislation that would centralize the federal cybersecurity systems and focus resources to prevent future breaches rather than merely imposing new criminal statutes, reporting requirements, and other bureaucratic measures.

Now is time for the Federal Government to acknowledge the failure of the existing cybersecurity infrastructure. This Comment advocates enacting legislation that would consolidate the management of all federal cybersecurity infrastructure under the U.S. Department of Homeland Security ("DHS"). Part I examines the shortcomings in the existing national cybersecurity policy framework leading to the failure of OPM and will discuss current legislative proposals and pending legislation regarding cybersecurity reform. Part II discusses the ever-increasing frequency and sophistication of cyber threats and the inability of federal infrastructure to face security challenges of a globalized cyberspace. The focus is particularly on breaches of government data and the failure of OPM to implement necessary infrastructure needed to prevent recurring data breaches. In Part III, this Comment looks to pending complaints filed by the affected individuals following the OPM Breach, as well as past instances where data breaches resulted in adjudication. Finally, Part IV concludes the United States cybersecurity policy must better manage federal data by: (1) suspending the current framework, and (2) by implementing a centralized cybersecurity framework that authorizes DHS to exercise regulatory and enforcement powers in order to combat domestic and foreign threats to the federal cyber-infrastructure.

I. BACKGROUND

On June 4, 2015, *The New York Times* broke a story revealing OPM experienced an almost year-long intrusion of the agency's information technology systems by unknown intruders.[15] OPM is the primary federal agency tasked with conducting and storing data related to the majority of federal background investigation used to gain security clearances.[16] This breach resulted in the exposure of at least four million former and current federal employees' personally identifiable information ("PII").[17] Despite this initial report, on June 12, 2015, the White House confirmed a second, more severe breach that occurred earlier in April 2015, which targeted the agency's database of employee back-

---

[15] David E. Sanger & Julie Hirschfeld Davis, *Hacking Linked to China Exposes Millions of U.S. Workers*, N.Y. TIMES (June 4, 2015), http://nyti.ms/1XsoDU6.

[16] *Id*.

[17] *Id.*

ground investigation records.[18]

While OPM initially projected only a small amount of records where compromised, an ongoing interagency investigation with DHS has "concluded with high confidence that sensitive information, including the Social Security Numbers (SSNs) of 21.5 million individuals, was stolen from the background investigation databases."[19] OPM's press release stated, "[t]his includes 19.7 million individuals that applied for a background investigation, and 1.8 million non-applicants, predominantly spouses or co-habitants of applicants…and approximately 1.1 million [files] include fingerprints."[20]

In the 21st century, the flow of globally-interconnected information, communications, and data stored across cyberspace[21] has become an integral part of the Federal Government's cyber-infrastructure.[22] To ignore the severe implications a breach poses to national security and economic prosperity would be grossly negligent.[23] Upon taking office, President Barack Obama claimed, "[o]ur digital infrastructure—the networks and computers we depend on every day—will be treated as they should be: as a strategic national asset."[24] However, since the President made this statement, subsequent breaches, hacks, and failures of the cyber-systems continue to underscore the failure to establish a cohesive strategy.[25] In order to realize the vast benefits of technological ad-

---

[18] Kate Vinton, *White House Confirms Second Government Data Breach Targeting Sensitive Military, Intelligence Personnel Data*, FORBES (June 12, 2015, 5:52 PM), http://onforb.es/1sNk63q; Michael D. Shear & Scott Shane, *White House Weighs Sanctions After Second Breach of a Computer System*, N.Y. TIMES (June 12, 2015), http://nyti.ms/1pAHqiM; David Bisson, *The OPM Breach: Timeline of a Hack*, TRIPWIRE (July 10, 2015, 9:00 AM), http://bit.ly/1qFw6lD.

[19] Press Release, U.S. Office of Personnel Mgmt., OPM Announces Steps to Protect Federal Workers and Others from Cyber Threats (July 9, 2015), http://1.usa.gov/1q3e7WL [hereinafter OPM - Steps to Protect Fed. Workers].

[20] *Id*.

[21] WHITE HOUSE, NATIONAL SECURITY PRESIDENTIAL DIRECTIVE-24, 3 (January 8, 2008), http://bit.ly/1RvBAXw ("'[C]yberspace' means the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.").

[22] *Id.* at 2.

[23] Tony Scott, *FACT SHEET: Enhancing and Strengthening the Federal Government's Cybersecurity*, THE WHITE HOUSE BLOG (June 17, 2015, 5:44 PM), http://1.usa.gov/1WMwt8N ("[C]ybersecurity risks pose some of the most serious economic and national security challenges of the 21st Century. Technologies and systems of the past cannot keep pace with rapidly evolving and persistent cyber threats.").

[24] Remarks on Securing the Nation's Information and Communications Infrastructure, 2009 Daily COMPILATION OF PRESIDENTIAL DOC., DCPD200900410, 3 (May 29, 2009).

[25] Letter from Sen. Ron Wyden, Chairman on Committee of Finance, to William Evanina, Director, Nat'l Counterintelligence and Sec. Ctr. 1 (Aug. 12, 2015), http://1.usa.gov/1Rn4WKX ("The fact that such sensitive information was not adequately protected raises real questions about how well the government can protect personnel information in the future, especially as the security clearance process moves toward conducting ongoing evaluations and incorporating publicly available electronic information….").

vancements, citizens must be informed and confident in the infrastructure in place keeping their information secure and preventing malicious infiltrations.[26] Furthermore, nation require public confidence of their digital infrastructure to secure sensitive data and protect national security.[27] This is not to say that any one policy-shift will prevent all malicious activity, but the nation's current cybersecurity strategy remains fragmented and its bureaucratic scheme disorganized, which only hinders the America's ability to engage other nation-states in meaningful dialogue to discourage cybercrime in all its forms.[28]

Cybersecurity will only continue to pose more challenges to policy makers as technology advances; malicious actors will continue to develop new methods to exploit networks, conduct cyber espionage, or compromise national security with greater ease.[29] Joel Brenner, a former senior counsel to the National

---

[26] Michael James Barton, *The 'Human' Factor is Key in Cybersecurity*, INSIDESOURCES (July 16, 2015), http://bit.ly/1U9Q6XV.

> The human factor has an important element: Policy. The policy governing computer access in an organization is critical—who has access to what, and when, and from where should be the cornerstone of a security plan. These policies determine who has access to what intellectual property, and who may access what information remotely, how many characters are required in a password, and a whole host of other elements critical to an organization's security posture.

Id.

[27] Kim Zetter & Andy Greenberg, *Why The OPM Breach Is Such a Security and Privacy Debacle*, WIRED (June 11, 2015, 10:40 PM), http://bit.ly/1Pu5UPN (quoting Chris Eng, Vice President of Research Veracode)

> 'It could be very damaging from a counterintelligence and national security standpoint'…SF-86 forms can include a list of foreign contacts with whom a worker has come in contact. Diplomats and other workers with access to classified information are required—depending on their job—to provide a list of these contacts. There is concern that if the Chinese government got hold of lists containing the names of Chinese nationals who had been in touch with US government workers, this could be used to blackmail or punish them if they had been secretive about the contact.

Id.

[28] Brendan Sasso, *Does NSA Spying Leave the U.S. Without Moral High Ground in China Hack?*, THE ATLANTIC (June 14, 2014), http://theatln.tc/1qFwC2Y ("[T]he U.S. is an awkward position in deciding how to respond to the humiliating blow. That's partially because in the two years since Edward Snowden's leaks about U.S. surveillance, the Obama administration has repeatedly argued that hacking into computer networks to spy on foreigners is completely acceptable behavior.").

[29] KRISTEN FINKLEA & CATHERINE A. THEOHARY, CONG. RESEARCH SERV., R42547, CYBERCRIME: CONCEPTUAL ISSUES FOR CONGRESS AND U.S. LAW ENFORCEMENT 1 (2015), http://bit.ly/1OT6flC; Ellen Nakashima & Lisa Rein, *Chinese Hackers go after U.S. Workers' Personal Data*, WASH. POST (July 10, 2015), http://wapo.st/21JAkol [hereinafter Nakashima II] (quoting Shawn Henry, former executive assistant director of the FBI's Criminal, Cyber, Response and Service Branch) ("If the Chinese government got access to that type of data, it would be a significant breach because the data would allow them to have very detailed information about people who hold very sensitive clearances….").

Security Agency, explained "[t]he Internet was not built for security, yet we have made it the backbone of virtually all private-sector and government operations, as well as communications."[30] However, this reality cannot simply absolve the government's obligation to protect sensitive information by implementing a centralized cybersecurity strategy and the development of secure cyber-infrastructure. In order to effectuate the goal securing the nation's critical infrastructure[31], it is necessary to enact cybersecurity legislation with authoritative guidance at the federal level regarding breach notification and mitigation for not only the private-sector, but also federal agencies following any cyber-attack.

In addition to the effective education and recruitment of users who are authenticated to use such systems, there must be a consolidation of oversight and management of the Federal Government's cyberspace under the supervision and authority of one centralized agency that actively monitors and implements necessary infrastructure upgrades. DHS and each agency's Office of the Inspector General were recently given more expanded advisory roles in assisting agencies in meeting their cybersecurity goals.[32] Yet, the evidence shows agencies' responsiveness ranges from slow to blatantly unresponsive in heeding issued warnings, recommendations, and audits—to the detriment of 21.5 million Americans with data stolen during the OPM Breach.[33] Under a centralized

---

30 Joel Brenner, *Nations everywhere are exploiting the lack of cybersecurity*, WASH. POST (Oct. 24, 2014), http://wapo.st/1pKCEA2 ("Pervasive connectivity has brought dramatic gains in productivity and pleasure but has created equally dramatic vulnerabilities. Huge heists of personal information are common, and cyber-theft of intellectual property and infrastructure penetrations continue at a frightening pace.").

31 U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-07-626T, CRITICAL INFRASTRUCTURE: CHALLENGES REMAIN IN PROTECTING KEY SECTORS 1-2 n.2 (2007); *see also* 42 U.S.C. § 5195c(e) ("'[C]ritical infrastructure' means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on national security, national economic security, and national public health or safety, or any combination of those matters.").

32 White House - Administration Cybersecurity Efforts 2015, *supra* note 11.

33 Memorandum from Patrick E. McFarland, Inspector General, Office of Personnel Mgmt., to Katherine Archuleta, Director, Office of Personnel Mgmt. 1 (June 17, 2015), http://1.usa.gov/1UQVT7m [hereinafter Memorandum from Inspector General McFarland to Director Archuleta]

> Our primary concern is that the [Office of the Chief Information Officer ("OCIO")] has not followed U.S. Office of Management and Budget (OMB) requirements and project management best practices. The OCIO has initiated this project without a complete understanding of the scope of OPM's existing technical infrastructure or the scale and costs of the effort required to migrate it to the new environment.

Id.; *Under Attack: Federal Cybersecurity and the OPM Data Breach: Hearing Before the S. Comm. on Homeland Sec. & Gov't Affs.*, 114th Cong. (June 25, 2015) [hereinafter *Under Attack - S. Comm. on Homeland Sec. & Gov't Affs.*] (statement of Patrick E. McFarland, Inspector General, Office of Personnel Mgmt.). ("Although OPM has made progress in certain areas, some of the current problems and weaknesses were identified as far back as

cybersecurity scheme headed by DHS, agencies ought be required to meet cybersecurity requirements and be held liable for disregarding necessary oversight and investment recommendations.

II. U.S. CYBERSECURITY POLICY: A SCATTERED FRAMEWORK

There is little doubt the revelation of the OPM Breach thrusted federal cybersecurity back into the spotlight.[34] The impetus has long been on expansion, modernization, and regulation of private-sector cyberspace rather than on securing the current, aging federal systems.[35] However, a review of the nation's cybersecurity policy as a whole reveals a fragmented framework of vague responsibilities that are delegated to various agencies as a means of combatting the expanding threat of cyber-attacks.[36] A centralized cybersecurity framework would involve both securing the federal cyber-infrastructure as well as assisting in the regulation of nonfederal systems.[37]

Fiscal Year (FY) 2007. We believe this long history of systemic failures to properly manage its IT infrastructure may have ultimately led to the breaches we are discussing today.")

[34] J.D. Harrison, *Will OPM Breach Spur Senate Action on Cybersecurity Information-Sharing Legislation?*, U.S. CHAMBER OF COMMERCE (June 19, 2015, 3:45 PM), http://uscham.com/1UokcJS.

[35] *See* ERIC A. FISHER, CONG. RESEARCH SERV., R42114, FEDERAL LAWS RELATING TO CYBERSECURITY: OVERVIEW AND DISCUSSION OF PROPOSED REVISIONS 1-2 (2013), http://bit.ly/1U7fE5c (listing recent congressional statutes that address cybersecurity and short summaries regarding how the statute affects cybersecurity).

[36] *Id.* at 4

> Under current law, all federal agencies have cybersecurity responsibilities relating to their own systems, and many have sector-specific responsibilities for critical infrastructure, such as the Department of Transportation for the transportation sector. Cross-agency responsibilities are complex, and any brief description is necessarily oversimplified. In general, in addition to the roles of White House entities, DHS is the primary civil-sector cybersecurity agency. NIST, in the Department of Commerce, develops cybersecurity standards and guidelines that are promulgated by OMB, and the Department of Justice is largely responsible for the enforcement of laws relating to cybersecurity. The National Science Foundation (NSF), NIST, and DHS all perform research and development (R&D) related to cybersecurity. The National Security Agency (NSA) is the primary cybersecurity agency in the national security sector, although other agencies also play significant roles. The recently established U.S. Cyber Command, part of the U.S. Strategic Command in the Department of Defense (DOD), has primary responsibility for military cyberspace operations.

Id.

[37] Aliya Sternstein, *Senators Want Homeland Security to be a Leading Cyberdefense Agency*, NAT'L J. (July 23, 2015).

> Just as CYBERCOM monitors and blocks threats to the military network, DHS, under proposed legislation, would scan for and repel attacks against the dot-gov domain. In the event of a suspected threat, the new 2015 Federal Information Security Management Reform Act lets DHS direct agencies ²to take any lawful action with respect to

However, the complexity of the current cybersecurity framework highlights the fragmented oversight and enforcement approaches across the public and private sectors,[38] which has led to various states' responses.[39] Contributing to the complexity, more than fifty federal statutes[40] currently bear the burden of codifying America's cybersecurity framework.[41] With such a fragmented approach to cybersecurity, the difficulties faced in implementing a centralized national policy and promoting meaningful cybersecurity standards with other nation-states should come as no surprise. Technology has progressed significantly in the last several decades, to the point where a system can be programmed and allowed to run with very little need for human interaction or supervision;[42] nevertheless, the reality is that the human component in securing data remains the largest contributor to breach, loss, and theft.[43] Furthermore, these advancements have given rise to the threat of hacking organizations, corporate espionage,[44] and state-sponsored government espionage.[45]

> the operation of the information system² at risk. IT systems subject to partial override, during emergencies, would include private-sector networks that handle government information. The bill also would task DHS with ²conducting targeted risk assessments and operational evaluations² of agency and contractor systems, including vulnerability scans.

Id.

38 See generally FED. TRADE COMMISSION, *supra* note 12, at 5.

39 FRANCESCA SPIDALIERI, PELL CTR. FOR INT'L. RELATIONS AND PUB. POLICY, STATE OF THE STATES ON CYBERSECURITY 7-8 (2015), http://bit.ly/1UPdBa9.

40 *See* Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-22 (2012) (prohibiting unauthorized electronic eavesdropping); E-Government Act of 2002, 44 U.S.C. § 101 (2012) (serving as the primary legislative vehicle to guide federal IT management and initiatives to make information and services available online, and includes various cybersecurity requirements); Federal Information Security Management Act of 2002, 44 U.S.C. §§ 3541, *et seq.* (2012) (clarifying and strengthening NIST and agency cybersecurity responsibilities, establishing a central federal incident center, and making OMB, rather than the Secretary of Commerce, responsible for promulgating federal cybersecurity standards); *see generally* FISHER, *supra* note 35, at 52-61 tbl.2 (listing the entire list of federal statutes concerning cybersecurity).

41 *See* FISHER, *supra* note 35, at 52-61 tbl.2.

42 Barton, *supra* note 26.

43 *Id.* ("Companies can no longer rely on software, hardware and security firewalls. Their employees are the target of the professional hackers, and are the network's weak link. Routine cybersecurity training paired with a robust review of policy provides the best defense of an organization's network.").

44 Charles Riley, *Xi Goes to Washington: 4 Problems for the U.S. and China*, CNN MONEY (Sept. 18, 2015, 2:52 AM), http://cnnmon.ie/22yU3gj ("Washington also says it has caught Chinese spies stealing blueprints and business plans. Last year, federal prosecutors took the unprecedented step of filing formal criminal charges against five Chinese government spies for breaking into Alcoa, U.S. Steel Corp., Westinghouse and others.").

45 Alan Spiress, *Computer System Under Attack*, WASH. POST (Oct. 6, 2006), http://wapo.st/1WMGhjb (noting in 2006 Chinese hackers breached the system of a sensitive Commerce Department Bureau of Industry and Security, "forcing it to replace hundreds of workstations and block employees from regular use of the Internet for more than a

Despite the ever evolving external threats associated with cybersecurity, the internal threats are most neglected and can easily cripple any policy framework that is not properly implemented or adhered to. A recent Government Accountably Office ("GAO") review of federal information security found there was a significant decrease in agencies reporting their users had received security awareness training in 2014.[46] The effective cornerstone of any policy recommendation on cybersecurity must focus on securing user access, system modification capabilities, and exfiltration sensitive federal data clearance, since these users remain the greatest risk to the proper function of any cybersecurity policy.[47]

Currently, the Federal Information Security Management Act of 2002 ("FISMA"), and its amended iterations are the primary means of codifying the government's approach to cybersecurity.[48] However, in the wake of the OPM Breach, the Obama Administration's own cybersecurity agenda together with pending legislative proposals before Congress fall short in synthesizing the United States' response to increasingly malicious cybersecurity threats.

A. The Federal Information Security Management Acts of 2002 and 2014

Under FISMA,[49] federal agencies are tasked with cybersecurity responsibilities relating to their own systems, while other responsibilities for cybersecurity functions are distributed among several other agencies.[50] The FISMA scheme tasks each agency head to provide "information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of" the agen-

---

month."); Ellen Nakashima, *Hackers Breach Some White House Computers*, WASH. POST (Oct. 28, 2014), http://wapo.st/1WMGhQe ("Hackers thought to be working for the Russian government breached the unclassified White House computer networks in recent weeks…").

46 U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-15-714, FEDERAL INFORMATION SECURITY: AGENCIES NEED TO CORRECT WEAKNESSES AND FULLY IMPLEMENT SECURITY PROGRAMS 37 (2015) [hereinafter GAO-15-714].

47 Barton, *supra* note 26; INST. FOR CRITICAL INFRASTRUCTURE TECH., HANDING OVER THE KEYS TO THE CASTLE: OPM DEMONSTRATED THAT ANTIQUATED SECURITY PRACTICES HARM NATIONAL SECURITY 21 (2015), http://bit.ly/1XRiC1e [hereinafter HANDING OVER THE KEYS TO THE CASTLE] ("Reform of the critical cybersecurity infrastructure as reformation of expertise of personnel, reformation of vulnerable, outdated technology, and reformation to end 25 years of poor cybersecurity practices can last far longer than 30 years and help to mitigate extenuating long-term consequences of the OPM's breach.").

48 Federal Information Security Management Act of 2002, 44 U.S.C. §§ 3541, *et seq.* (2012).

49 *Id*.

50 HOUSE REPUBLICAN CYBERSECURITY TASK FORCE, TASK FORCE RECOMMENDATIONS 13 (2011), http://1.usa.gov/1VLiL7I ("FISMA is the main law governing the federal government's information security program.").

cy's information or information systems.[51] In addition, the legislation requires federal agencies to develop, document, and implement an agency-wide information security program.[52] Often such tasks are designated to the Chief Information Officer ("CIO") within each agency.[53] Under current law, in addition to its budgetary role in federal cybersecurity efforts, the Office of Management and Budget ("OMB") possesses the primary responsibility for promulgating and enforcing information security requirements under FISMA for federal information systems for many federal agencies and most notably OPM.[54]

FISMA requires agencies provide security awareness training to personnel, including contractors and other users of information systems that support the operations and assets of the agency.[55] This scheme provides guidelines to agencies regarding information security risks associated with their operational activities and details the responsibilities each agency possesses—yet falls short of centralizing oversight authority to one particular agency in order to protect national security.[56] FISMA also requires agencies to train and oversee personnel who have significant information security responsibilities.[57] While the number of individuals with significant security responsibilities has decreased in 2014, there has been an increase in user and contractor related breach incidents that call into question whether agencies are doing enough to properly train individuals.[58]

In April 2015, the Department of Veterans Affairs' Office of Inspector General reported two contractors had improperly accessed the agency's network from foreign countries using personally owned equipment.[59] In February 2015,

---

51 Federal Information Security Management Act of 2002, 44 U.S.C. § 3543 (2012).

52 *Id.* § 3544(a).

53 *Id.* § 3544.

54 ERIC A. FISHER, CONG. RESEARCH SERV., R43831, CYBERSECURITY ISSUES AND CHALLENGES: IN BRIEF 3 (2014), http://bit.ly/1YT5dX6; *The Expanding Cyber Threat: Hearing Before the Subcomm. on Res. & Tech. of the H. Comm. on Sci., Space & Tech.*, 114th Cong. 66 (2015) (statement of Eric A. Fisher, Senior Specialist in Science & Technology, Congressional Research Service).

55 GAO-15-714, *supra* note 46, at 7.

56 FINKLEA ET AL., *supra* note 14, at 6 ("FISMA largely does not apply to national security systems, which fall under the Committee on National Security Systems."); Richard W. Walker, *FISMA Security Approach Falls Short, Fed IT Pros Say*, INFORMATIONWEEK DARKREADING (Sept. 25, 2013), http://ubm.io/25izs1d (according to a 2013 OMB survey, only 27% of federal agencies reported that their agencies are "currently perfectly compliant" with FISMA).

57 U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-13-776, FEDERAL INFORMATION SECURITY: MIXED PROGRESS IN IMPLEMENTING PROGRAM COMPONENTS; IMPROVED METRICS NEEDED TO MEASURE EFFECTIVENESS 16 (2013), http://1.usa.gov/244Y0EO.

58 U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-14-612, INFORMATION SECURITY: AGENCIES NEED TO IMPROVE OVERSIGHT OF CONTRACTOR CONTROLS 17 (2014), http://1.usa.gov/1THdTjr.

59 OFFICE OF INSPECTOR GEN., DEP'T OF VETERANS AFFAIRS, REPORT NO. 13-01730-159,

the Director of National Intelligence stated that unauthorized computer intrusions were detected on the networks of OPM and two of its contractors.[60] The contractors were processing sensitive PII, related to national security clearances for federal employees. While these instances stand apart from otherwise unknown actors that caused the OPM Breach, one contractors has been implicated in the breach.[61] The GAO's focus on cybersecurity training for users clearly highlights one of the more fundamental recommendations that agencies must implement in order to become better prepared to combat cybersecurity threats.[62] Providing training for agency personnel is critical to securing systems and information because people are one of the weakest links when securing systems and networks.

In the wake of these security incidents, Congress passed an updated Federal Information Security Modernization Act of 2014,[63] ("FISMA 2014") which was signed into law by President Obama in December 2014.[64] This legislation was the first attempt in more than a decade by the Federal Government toward delegating agency tasks with regard to cybersecurity and data protection.[65] As amended, FISMA 2014 still requires federal agencies to implement agency-wide cybersecurity programs to protect sensitive data and information, extending such requirements to service and systems provided or managed by another agency, contractor, or outside source.[66] However, FISMA 2014 expands authorization to include DHS, by tasking them to assist OMB with oversight and regulation of agencies' implementation of cybersecurity programs, operate the federal information security incident center ("US-CERT"), and provide agencies with operational and technical assistance for continuously monitoring and mitigating cyber vulnerabilities ("EINSTEIN").[67]

Codifying a set of directives outlined in 2010 from the Obama Administra-

---

ADMINISTRATIVE INVESTIGATION: IMPROPER ACCESS TO THE VA NETWORK BY VA CONTRACTORS FROM FOREIGN COUNTRIES 2 (2015), http://1.usa.gov/1XRkiYs.

60 *Worldwide Threat Assessment of the U.S. Intelligence Community: Hearing Before the S. Comm. on Armed Servs.,* 114th Cong. (Feb. 9, 2015), http://1.usa.gov/25iz6rd (statement of James Clapper, Director of National Intelligence).

61 Aaron Boyd, *Contractor breach gave hackers keys to OPM data*, FED. TIMES (June 25, 2015, 4:44 PM), http://bit.ly/1RllYnW.

62 GAO-15-714, *supra* note 46, at 27.

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

64 Press Release, White House, Office of the Press Sec'y, Statement by the Press Secretary Bills Signed into Law (Dec. 18, 2014), http://1.usa.gov/1XXgSDJ.

65 Sean B. Hoar, *Congress Passes the Federal Information Security Modernization Act of 2014: Bringing Federal Agency Information Security into the New Millennium*, PRIV. & SEC. L. BLOG (Dec. 18, 2014), http://bit.ly/1MoBMLf.

66 GAO-15-714, *supra* note 46, at 11.

67 *Id*. at 11.

tion's cybersecurity policy objective, the FISMA 2014 gives DHS operational authority to oversee implementation of federal cybersecurity systems, including the authority to issue binding operational directives[68] and set requirements for breach notification within federal agencies.[69] In addition, agency CIOs were provided with additional budgeting and program authorities.[70] In addition to the advisory roles played predominately by OMB and DHS, other agencies such as the National Institute of Science and Technology ("NIST"), played a critical role in issuing and updating security standards and guidelines for information systems utilized by Federal agencies.[71] Despite these updates, the OPM Breach reveals how little impact such changes have had in impacting the government's approach to these real, ever present threats.

B. Current Legislative Proposals

Several bills concerning cyber threats have been proposed by the current Congress, although all stagnated in Spring 2015.[72] Nevertheless, in the wake of the OPM Breach, legislators have called for a renewed push toward meaningful reform on cybersecurity.[73] While much progress was made during Summer 2015 on amending these cyber-related bills, many have cautioned that the cur-

---

[68] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (2014) (codified as amended at 44 U.S.C. § 3552(b)(1)).

> The term "binding operational directive" means a compulsory direction to an agency that is for the purposes of safeguarding Federal information and information systems from a known or reasonably suspected information security threat, vulnerability or risk.

Id.

[69] Memorandum from Peter R. Orszag & Howard A. Schmidt to the Heads of Executive Departments and Agencies 2 (July 6, 2010), http://1.usa.gov/1UokNvg (delegating responsibilities to DHS in 2010).

[70] 40 U.S.C. § 11319 (2014).

[71] *See* ELAINE BARKER ET AL., NAT'L INST. OF STANDARDS & TECH., SPECIAL PUB. 800-56B, RECOMMENDATION FOR PAIR-WISE KEY-ESTABLISHMENT SCHEMES USING INTEGER FACTORIZATION CRYPTOGRAPHY, at ii (2014), http://1.usa.gov/1XRkRSg ("NIST is responsible for developing information security standards and guidelines, including minimum requirements for Federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate Federal officials exercising policy authority over such systems.").

[72] RITA TEHAN, CONG. RESEARCH SERV., R43317, CYBERSECURITY: LEGISLATION, HEARINGS, AND EXECUTIVE BRANCH DOCUMENTS 2 (2015), http://bit.ly/1Ts7fPH ("More than 20 bills have been introduced in the 114th Congress that would address several issues, including data-breach notification, incidents involving other nation-states, information sharing, law enforcement and cybercrime, protection of critical infrastructure (CI), workforce development, and education.").

[73] INST. FOR CRITICAL INFRASTRUCTURE TECH., MOVING FORWARD: HOW VICTIMS CAN REGAIN CONTROL AND MITIGATE THREATS IN THE WAKE OF THE OPM BREACH 3-4 (2015), http://bit.ly/1XRiC1e [hereinafter MOVING FORWARD].

rent proposals remain disproportionally focused on: breach notifications, information sharing and private sector enforcement rather than on agency jurisdiction, oversight authority, and infrastructure protection.[74]

The House of Representatives bills—originally labeled H.R. 1560: Protecting Cyber Networks Act ("PCNA"); and H.R. 1731: the National Cybersecurity Protection Advancement Act of 2015 ("NCPAA")—passed the House during the week of April 20, 2015 and were consolidated, with the PCNA becoming Title I and the NCPAA Title II of H.R. 1560.[75] Both these bills focus on the sharing of cyber threat information within the private sector, and between the private sector and government, creating a structure for the information-sharing process; and further address issues like consumer privacy, individual civil liberties with regard to PII, and the liability risks of private-sector sharing.[76]

In the Senate, S. 754, the Cyber Information Sharing Act of 2015 ("CISA"), and S. 456, The Cyber Threat Sharing Act of 2015 ("CTSA"), have been combined under S. 754.[77] The bill was long stalled in the Senate, but passed in October 2015.[78] Following the OPM Breach revelation, the White House was quick to endorse this effort by suggesting the Senate bill improved on earlier efforts—both in the protection of PII and better intimations on the allowed uses of personal information.[79] However, there was intense opposition to S. 754 from civil liberties, privacy advocates, some legislators, and even from the DHS itself.[80] Senator Al Franken [D-MN] warned the sharing provisions of the bill, "could sweep away important privacy protections."[81] The opposition re-

---

74 *See* Bryan Thompson & Sean B. Hoar, *2015 Data Breach Legislation Six Month Review: Many Proposals, Few Changes*, PRIV. & SEC. L. BLOG (July 8, 2015), http://bit.ly/1TSIbvH ; Katie Bo Williams, *Six Cybersecurity Lawmakers to Watch in 2016*, THE HILL (Dec. 28, 2015, 6:05 AM), http://bit.ly/1RppVLM; Katie Bo Williams, *House Passes Bill Mandating DHS Cybersecurity Strategy*, THE HILL (Oct. 6, 2015, 5:52 PM), http://bit.ly/1VLmmCV.

75 ERIC A. FISHER, CONG. RESEARCH SERV., R44069, CYBERSECURITY AND INFORMATION SHARING: COMPARISON OF H.R. 1560 (PCNA AND NCPAA) AND S. 754 (CISA) 3 (2015), http://bit.ly/1TSIjLA.

76 ERIC A. FISHER & STEPHANIE M. LOGAN, CONG. RESEARCH SERV., R43996, CYBERSECURITY AND INFORMATION SHARING: COMPARISON OF H.R. 1560 AND H.R. 1731 AS PASSED BY THE HOUSE 2-3 (2015), http://bit.ly/1Tvl7DH.

77 Taylor Armerding, *Cybersecurity Legislation Still Draws Intense Opposition*, CIO (Sept. 23, 2015, 7:08 AM), http://bit.ly/1pKNRAs.

78 *See S.754 – Cybersecurity Information Sharing Act of 2015*, Congress.gov (last visited Mar. 7, 2016), http://1.usa.gov/1U9Rjyr.

79 Cory Bennet, *White House Endorses Senate Cyber Bill*, THE HILL (Aug. 4, 2015, 5:29 PM), http://bit.ly/1T9BGZl.

80 Eric Geller, *Sen. Ron Wyden thinks the next big cybersecurity bill could make things worse*, THE DAILY DOT (Sept. 14, 2015, 9:30 AM), http://bit.ly/1TSIg2r.

81 Sen. Al. Franken, *Remarks of Sen. Al Franken on the Cybersecurity and Information Sharing Act of 2015*, SEN. AL FRANKEN (Oct. 22, 2015), http://1.usa.gov/1SfR29O; *see also*

sulted in more than a hundred amendments, only three of which were ultimately agreed upon, drawing even more opposition of the bill to protect privacy.[82]

One such amendment, which could seemingly keep the impetus on cybersecurity reform in the congressional forefront is S. 1828, the Federal Information Security Management Reform Act of 2015, would directly tackle federal cybersecurity issues raised with the OPM Breach.[83] Several senators have even gone so far as to publicly endorse a revamping of cybersecurity policy that would put DHS in charge.[84] Senator Susan Collins [R-ME], who co-sponsored S. 1828, stated at its introduction:

At present, DHS does not have the authority to monitor the networks of government agencies unless they have permission from that agency. DHS also cannot regularly deploy countermeasures to block malware without permission from the agency. This limited authority hinders the security of .gov information systems which – as evidenced by the recent OPM attack – contain highly sensitive personal data such as Social Security numbers, home addresses, dates of birth, and in some cases, extensive background information of federal employees, retirees, and contractors.[85]

In total, S. 1828 addresses five key policy areas to combatting future cyberattacks by: (1) allowing DHS to operate intrusion detection and prevention capabilities on all federal agencies on the ".gov domain;"[86] (2) direct DHS to conduct risk assessments of any network within the government domain;[87] (3) give the Secretary of DHS authority to operate defensive countermeasures on these agency networks once a cyber threat has been detected;[88] (4) strengthen and streamline the authority Congress gave to DHS last year to issue binding operational directives to federal agencies, especially to respond to substantial

---

114 Cong. Rec. S7498 (daily ed. Oct. 27, 2015).

82 *See S.754–Cybersecurity Information Sharing Act of 2015*, Congress.gov (last visited Mar. 7, 2016), http://1.usa.gov/1U9Rjyr; Mike Masnick, *Senate Rejects All CISA Amendments Designed to Protect Privacy, Reiterating That It's a Surveillance Bill*, TECHDIRT (Oct. 27, 2015, 11:40 AM), http://bit.ly/1RkiczY.

83 Aaron Boyd, *New Bill Strengthens DHS Role in Federal Cybersecurity*, FED. TIMES (July 23, 2015, 11:08 AM), http://bit.ly/1VNDEPU.

84 Cory Bennett, *Senators unveil new Homeland Security cyber bill*, (July 22, 2015, 9:14 AM), http://bit.ly/1UQPLef (statement of Sen. Susan Collins) ("While the Department of Homeland Security has the mandate to protect the .gov domain, it has only limited authority to do so.").

85 Press Release, Sen. Kelly Ayotte, Following Cyber Attack at OPM, Ayotte and Colleagues Introduce Bipartisan Cybersecurity Bill, (July 22, 2015), http://1.usa.gov/1UW32Cg.

86 Federal Information Security Management Reform Act of 2015 § 2, S. 1828, 114th Cong. (2015).

87 *Id.*

88 *Id.*

cybersecurity threats in emergency circumstances;[89] and (5) require the OMB to report to Congress annually on the extent to which it has exercised its existing authority to enforce government-wide cybersecurity standards.[90]

While the co-sponsors of the bill suggest the proposal is a proper fix to the procedural problems that led to the devastating OPM Breach, others have decried it as a simple codification of the role DHS has already tried to take in light the increased threat of cyber-attacks in the last decade.[91] This is not to say that legislatively authorizing DHS with centralized authority will not be the first step in streamlining the process of securing the nation's cyber-infrastructure. Unfortunately, this legislation does not authorize the DHS to take control of agency networks during cyber-emergencies nor does it define what a cyber-emergency might constitute.[92] Senator Mark Warner [D-VA] has stated,

The attack on OPM has been a painful illustration of just how behind the curve some of our federal agencies have been when it comes to cybersecurity…If we want to be better prepared to meet this threat in the future, we have to make sure that the [DHS] has the tools it needs to adequately secure our federal civilian networks.[93]

C. The Administrative Approach – Executive Orders and Political Banter

Since taking office, President Barack Obama has touted the work that his Administration has done in regard to securing the nation's cyberspace.[94] Immediately after taking office, President Obama announced his plan to tackle cybersecurity issues.[95] While such plans shifted in the subsequent years, in

---

89 *Id.*

90 *Id.*

91 Senator Susan M. Collins, Statement on S. 1828, (July 22, 2015), http://bit.ly/1XOpRtg.

92 Sternstein, *supra* note 37.

93 Press Release, Sen. Mark Werner, Following Cyber Attack at OPM, Warner & Collins Introduce Bipartisan Bill to Improve Government Cybersecurity (July 22, 2015), http://1.usa.gov/1UwgEpf.

94 White House - Administration Cybersecurity Efforts 2015, *supra* note 11 ("As the cyber threat continues to increase in severity and sophistication, so does the pace of the Administration's efforts. Included in this fact sheet are some of the achievements of this Administration in just the last six months.").

95 Tony Scott, *FACT SHEET: Enhancing and Strengthening the Federal Government's Cybersecurity*, The White House: Blog (June 17, 2015, 5:44 PM), http://1.usa.gov/1WMwt8N.

> In 2009, President Obama named the first Cybersecurity Coordinator and directed a comprehensive Cyberspace Policy Review to assess U.S. policies and structures for cybersecurity. Since then, the Administration has taken a number of aggressive ac-

2015, the President released Executive Order regarding cybersecurity threats in the wake of increasing private sector breaches[96] and most recently issued Executive Order 13694, which authorizes the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, to impose financial sanctions on individuals and entities whose malicious cyber-enabled activities have contributed to a significant threat to the national security, foreign policy, economic health, or financial stability of the United States.[97] A move lauded as a strong political maneuver sharply directed at those engaging in state-sponsored or government espionage.[98]

Even as recently as July 2015, following the OPM Breach, OMB was directed to launch a 30-day Cybersecurity Sprint to assess and improve the health of all federal assets and networks, both civilian and military.[99] As part of this "Sprint," OMB ordered agencies to further protect federal information, improve the resilience of its networks, and report on their successes and challenges.[100] Agencies were instructed to immediately patch critical vulnerabilities, review and tightly limit the number of privileged users with access to authorized systems, and introduce strong authentication, especially for privileged

---

> tions to upgrade the Federal Government's technology infrastructure and protect government networks and information, implementing tools and policies in order to detect and mitigate evolving threats.

Id.

96 Exec. Order No. 13691, 80 Fed. Reg. 9,349, 9,349 (Feb. 20, 2015).

> In order to address cyber threats to public health and safety, national security, and economic security of the United States, private companies, nonprofit organizations, executive departments and agencies (agencies), and other entities must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible.

Id.

97 Exec. Order No. 13694, 80 Fed. Reg. 18,077, 18,077 (Apr. 2, 2015) ("[T]he increasing prevalence and severity of malicious cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States."); Press Release, Office of the Press Secretary, White House, Presidential Statement on Executive Order "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities" (April 1, 2015), http://1.usa.gov/1XOpZZP ("As we have seen in recent months, these threats can emanate from a range of sources and target our critical infrastructure, our companies, and our citizens. This Executive order offers a targeted tool for countering the most significant cyber threats that we face.").

98 Robert Hackett, *Sanctions: America's best new weapon against cyber crime,* FORTUNE (Apr. 2, 2015, 9:47 AM), http://for.tn/1sNlFP9.

99 Scott, *supra* note 23 ("United States Chief Information Officer (CIO) Tony Scott recently launched a 30-day Cybersecurity Sprint. As part of the effort, the Federal CIO has instructed Federal agencies to immediately take a number of steps to further protect Federal information and assets and improve the resilience of Federal networks.").

100 *Id*.

users.[101] All of these actions reduce the risk of adversaries penetrating federal networks. While the policy goals won political points in the news cycle, at a time when some federal employees were just beginning to be notified that their private information had been compromised, the excitement has wore thin with the high-level administration officials, and the mess has since been left to the agency heads and congressional committees to figure out how to grasp and reconcile the remain difficult issues.[102]

III. AGING INFRASTRUCTURE AND THE INCREASING THREAT OF FEDERAL DATA BREACHES

Despite the various efforts to implement a cybersecurity policy for the nation, the reality is technology has advanced far faster in the last decade than the Federal Government's ability to regulate and protect these systems.[103] Since 2006, the number cybersecurity incidents related to federal systems has increased exponentially, severely calling into question the effectiveness of the government's current approach to data protection.[104] According to the GAO and US-CERT, 5,503 incidents were reported in 2006 compared to 67,168 reported in 2014—an increase of more than 1,100 percent.[105] This increase in reported incidents is staggering considering the amount of money and resources spent by the Federal Government on information technology and cybersecurity infrastructure. Some have begun to question as to whether the investment has been worth the return.[106]

---

[102] Bob Gourley, *List of Cyber Threat "Wake-Up Calls" Growing: Policy makers have been hitting the snooze button since 1970,* CTO VISION, (June 7, 2015), http://bit.ly/1Xsqicf ("Our history indicates cyber security events frequently cause action and remediation and get widespread attention. But soon after the attempt to remediate, organizations collectively forget about the threat.").

[103] Shawn Zeller, *Congress Fails to Keep Up with Rapid Technology Advances*, CHI. TRIB. (Sept. 15, 2015, 12:20 PM), http://trib.in/22L1cql; *see also* Vivek Wadhwa, *Laws and Ethics Can't Keep Pace with Technology*, TECH. REV. (Apr. 15, 2014), http://bit.ly/20spcfM.

[104] Eli Dourado & Andrea Castillo, *Federal Cybersecurity Breaches Mount Despite Increased Spending*, MERCATUS CTR. (Jan. 20, 2015), http://bit.ly/1RDMX54.

> After more than a decade of billion dollar investments and government-wide information sharing, in 2013 'inspectors general at 21 of the 24 agencies cited information security as a major management challenge for their agency, and 18 agencies reported that information security control deficiencies were either a material weakness or significant deficiency in internal controls over financial reporting.

Id.

[105] U.S. GOV'T ACCOUNTABILITY OFFICE., GAO-15-725T, RECENT DATA BREACHES ILLUSTRATE NEED FOR STRONG CONTROLS ACROSS FEDERAL AGENCIES 3-4 fig.1 (2015), http://1.usa.gov/25ozuSH [hereinafter GOA-15-725T].

[106] Dourado, *supra* note 104.

The Federal Budget for Fiscal Year 2016 allocates $14 billion on cybersecurity.[107] President Obama requested $12.5 billion in 2015, which is roughly ten percent less; yet, the figure is almost 35 percent more than was spent in Fiscal Year 2014.[108] The federal cybersecurity budget represents about 16 percent of the total federal information technology budget of $86.4 billion for 2016, compared to the four percent that private companies typically allocate for the same purpose.[109]

DHS has allotted a large portion of its 2016 Budget—$582 million—for the EINSTEIN intrusion detection system, continuous diagnostics programs, and mitigation programs alone in order to continue the progress that has been made in deploying early detection systems across various federal agency networks.[110] The latest EINSTEIN intrusion detection iteration, EINSTEIN 3 Accelerated or "E3A" is particularly of interest because it is purportedly capable of detecting the types of intrusions that occurred at OPM.[111] While the system has been functional for a short while, DHS has been unsuccessful at securing its implementation across the federal agency network; the agency remains confident it will continue to expand the systems reach in order to detect future threats.[112]

---

[107] OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, FISCAL YEAR 2016 BUDGET OF THE U.S. GOVERNMENT 16 (2016), http://1.usa.gov/1XSXF66 [hereinafter OMB - FY 2016 BUDGET]; *see also* Office of Mgmt. & Budget, *The President's Budget for Fiscal Year 2017*, EXEC. OFFICE OF THE PRESIDENT, http://1.usa.gov/1ZAS7yy (Mar. 17, 2016) [hereinafter OMB - *The President's Budget for FY 2017*] (allocating $19 billion for cybersecurity)

[108] Jaikumar Vijayan, *Despite billions spent, US federal agencies struggle with cybersecurity*, CHRISTIAN SCI. MONITOR (June 10, 2015), http://bit.ly/1obxz1S.

[109] OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, ANALYTICAL PERSPECTIVES: BUDGET OF THE U.S. GOVERNMENT FISCAL YEAR 2016, at 281 (2016), http://1.usa.gov/1RkzJIk; PRICEWATERHOUSECOOPERS, MANAGING CYBER RISKS IN AN INTERCONNECTED WORLD: KEY FINDINGS FROM THE GLOBAL STATE OF INFORMATION SECURITY SURVEY 2015, at 19 (2014), http://pwc.to/21OpRrV.

[110] OFFICE OF MGMT. & BUDGET, ANNUAL REPORT TO CONGRESS: FEDERAL INFORMATION SECURITY MANAGEMENT ACT 6 (2015), http://1.usa.gov/1T9FfyF ("The President's FY 2016 Budget also invests $582 million to drive continued progress through CDM and EINSTEIN to enable agencies to detect and prevent evolving cyber threats.").

[111] *Under Attack - S. Comm. on Homeland Sec. & Gov't Affs.*, *supra* note 42 (written statement of Dr. Andy Ozment, Assistant Secretary, Office of Cybersecurity & Communications, National Protection and Programs Directorate); *see also* Jeh Charles Johnson, Secretary of Homeland Security, Securing The .Gov, Remarks Before the Center for Strategic and International Studies (July 8, 2015), http://1.usa.gov/22L3WUN [hereinafter Johnson - Securing The .Gov]("E3A has the capacity to both identify and block known malicious traffic…one key value of E3A is that it is an intrusion detection and prevention system that uses classified information to protect unclassified information.").

[112] Johnson - Securing The .Gov, supra note 111

> By December 2014, E3A protected 237,414 federal personnel. Today, E3A protects over 931,000 federal personnel, or approximately 45% of the federal civilian government. I have directed that DHS make E3A fully available to all federal departments and agencies, and have challenged us to make aspects of E3A available to all federal

Had EINSTEIN been deployed at OPM, some have suggested the intrusions could have been detected sooner, if not thwarted completely.[113]

Despite the federal expenditure on cybersecurity, the risks for many federal agencies appear to be getting worse.[114] DHS Secretary Jeh Johnson recently testified:

> To be frank, our federal .gov [domain] cybersecurity, in particular, is not where it needs to be…There is a great deal that has been done and is being done now to secure our networks. We do, in fact, block a large number of intrusions and exfiltrations, including those by state actors. But much more must be done.[115]

While budget concerns continually have resulted in blame from all sides of the aisle, increased expenditure on cybersecurity infrastructure "does not mean that all agencies have benefited equally from the largesse."[116] The Department of Defense ("DOD") and DHS have been the largest recipients of federal cybersecurity budgets. With $14 billion set aside for cybersecurity in the 2016 Federal Budget, approximately $5.5 billion is allocated to the DOD.[117]

Even in 2014, "the DOD and the DHS alone accounted for $10.3 billion of the total $12.7 billion in IT [information technology] security spending reported by federal agencies."[118] In the 2016 budget, DHS is getting a small increase of $7 million to its $473 million allotment for preventing malicious cyber activity against government agencies, and an additional $102.6 million to its $722 million budget for detecting, analyzing, and mitigating threats on behalf of other agencies.[119] Despite these budget increases, OPM dedicated only a combined $7 million to these two categories of tasks in 2014, even though the agency stores the PII of 32 million federal employees, more than most other federal agencies.[120] While budgeting concerns must always remain at the fore-

---

civilian departments and agencies by the end of 2015.

Id.

113 Suz Redfearn, *Einstein efforts accelerate under the spotlight of OPM breach*, FED. TIMES (Aug. 10, 2015, 8:35 PM), http://bit.ly/1U7fQRS.

114 GOA-15-725T, *supra* note 105.

115 *Worldwide Threats and Homeland Security Challenges: Hearing Before the H. Comm. on Homeland Sec.,* 114th Cong. (Oct. 21, 2015), http://1.usa.gov/1pEIhPt (statement of Jeh Johnson, Secretary of Homeland Security) (referring to cybersecurity across all .gov websites and noting that all .gov websites are subject to increasing threats and are not adequately protected).

116 Vijayan, *supra* note 108.

117 Sternstein, *supra* note 37; OMB - FY 2016 BUDGET, *supra* note 107, at 16; *see also* OMB - *The President's Budget for FY 2017*, *supra* note 107.

118 Vijayan, *supra* note 108.

119 *Fact Sheet: Department of Homeland Security Fiscal Year 2016 Budget*, DEP'T OF HOMELAND SEC. (February 2, 2015), http://1.usa.gov/1UW2nkc.

120 Mohana Ravindranath, *Before Breach, OPM Requested Millions of Dollars to Upgrade Network Security*, NEXTGOV (June 5, 2015), http://bit.ly/1U9ROsm ("OPM's 2016 budget request, released in February, proposed an additional $21 million in funding to 'im-

front of any enterprise—federal or civilian—the priority is and must remain the implementation of a policy framework that ensures centralized cybersecurity management. The various incidents in the last several years should ring alarm bells and demonstrates as how aging infrastructure and fragmented management have crippled the systems tasked with protecting highly sensitive data.

A. 2015: The Year of the Breach

In 2014, the GAO reported that 67,168 incidents were reported by federal agencies.[121] Given the growth in scope and scale of the cyber risks, it is no surprise that 2015 has given rise four significant incidents that highlight the failure of the current framework.[122] Beginning in late-2014, the United States Postal Service reported its information technology ("IT") systems had been compromised and the data of nearly 800,000 employees had been exposed.[123] In April 2015, the Department of Veteran Affairs announced that uncredentialed access had occurred to its network.[124] In June 2015, the IRS publically disclosed a breach of taxpayer information exposed the records of nearly 330,000 individuals, with potentially more affected.[125] Even before the June 2015 revelation of the largest breach in U.S. history that compromised OPM's network, the Director of National Intelligence revealed in February 2015 that they suspected unauthorized computer intrusions by outside contractors on the OPM network dating back to early 2014.[126]

---

plement and sustain agency network upgrades' first initiated in fiscal 2014 and 'security software maintenance to ensure a stronger, more reliable and better protected OPM network architecture.'").

[121] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-15-758T, INFORMATION SECURITY: CYBER THREATS AND DATA BREACHES ILLUSTRATE NEED FOR STRONGER CONTROLS ACROSS FEDERAL AGENCIES (2015), http://1.usa.gov/1obAkQV [hereinafter GAO-15-758T].

[122] *Id*. at 7, figure 1.

[123] *Id*. at 9; *see also* Laura Stevens, et al., *U.S. Postal Service Says It Was Victim of Data Breach*, WALL ST. J. (Nov. 10, 2014, 12:40 PM), http://on.wsj.com/1ZAXxJO.

[124] GAO-15-758T, *supra* note 121, at 8; *see also* Stevens, *supra* note 123.

[125] *Unauthorized Attempts to Access Taxpayer Data: Hearing Before the S. Comm. on Fin.*, 114th Cong. (June 2, 2015), http://1.usa.gov/1UVt4Wj (written statement of John Koskinen, Comissioner, Internal Revenue Service) ("As they continued to investigate, our team determined that a total of approximately 200,000 suspicious attempts to gain access to taxpayer information on the Get Transcript application had been made between mid-February and mid-May.").

[126] JAMES R. CLAPPER, OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, STATEMENT FOR THE RECORD: WORLDWIDE THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY 1-2 (2015), http://1.usa.gov/20spyDp.

B. OPM—The Largest Hack in U.S. History

In June 2015, OPM publically reported a cyber intrusion—allegedly by Chinese hackers[127]—that affected personnel records of over four million current and former federal employees.[128] OPM, under then-Director Katherine Archuleta, then announced that a separate incident may have compromised OPM systems relating to databases on background investigations conducted for security clearance.[129] Despite the fallout from the incident, diminished public perception of the agency, and congressional calls for leadership change at OPM[130], the Obama Administration defended the actions of OPM and Director Archuleta.[131] Reports issued in the subsequent weeks suggested the total number of affected federal employees could be much higher, and in early July 2015, OPM admitted that as many as 21.5 million past, current, and prospective federal employees had been affected by the breach, as well as other individuals for whom a federal background investigations were conducted.[132]

Congressman Jason Chaffetz [R-UT], Chairman of the House Committee on Oversight and Government Reform, has led the congressional charge in challenging OPM regarding its negligent behavior and failed implementation of compliant cybersecurity measures.[133] Since the revelation of the Breach, several congressional inquiries have led to new information surrounding the events of the OPM Breach, most recently revealing that 5.6 million fingerprints were additionally stolen.[134] In response to the increased number of compromised

---

127 Tian Shaohui, *Op-Ed: Irresponsible Remarks on China's Hacking Another Case of Habitual U.S. Slander*, NEW CHINA (June 5, 2015, 3:49 PM), http://bit.ly/1q9XCIu (dismissing the allegations of Chinese involvement as "obviously another case of Washington's habitual slander against Beijing on cyber security"); *see generally* 161 CONG. REC. S4065 (daily ed. June 11, 2015) (statement of Sen. Harry Reid).

128 FINKLEA ET AL., *supra* note 14, at 1-2.

129 *Id*.

130 Hurd, *supra* note 13 ("The refusal at the Office of Personnel Management to take responsibility and move swiftly to address significant deficiencies leads to only one conclusion. Accountability starts at the top. It's time for a change in leadership at the OPM."); *see also* Joe Davidson, *OPM Chief Berated at Hearing; Chairman Calls for Her Head*, WASH. POST (June 16, 2015), http://wapo.st/1sNllzG.

131 *Press Briefing by Press Secretary Josh Earnest*, WHITE HOUSE (June 17, 2015), http://1.usa.gov/1UvPsXQ ("Director Archuleta, in one of her first priorities that she identified after taking that job, was to upgrade the OPM computer network, particularly their cyber defenses. And this is obviously an ongoing process, and the President does have confidence that she is the right person for the job.").

132 OPM - Steps to Protect Fed. Workers, *supra* note 19.

133 Davidson, *supra* note 130; *see also* Joe Davidson, *OPM Director Survives Congressional Inquisition, For Now*, WASH. POST (June 25, 2015), http://wapo.st/1U7fxqd.

134 Press Release, Office of Personnel Mgmt., Statement by OPM Press Secretary Sam Schumach on Background Investigations Incident (Sept. 23, 2015), http://1.usa.gov/21NYy0E; *see*, *e.g.*, 114 CONG. REC. D797 (daily ed. July 8, 2015); 114

fingerprints, Chairman Chaffetz stated:

OPM keeps getting it wrong. This breach continues to worsen for the 21.5 million Americans affected. I have zero confidence in OPM's competence and ability to manage this crisis. OPM's [information technology] management team is not up to the task. They have bungled this every step of the way.[135]

Information released in June 2015 regarding the initial hack of OPM's network indicates that hackers gained access to employees' personal information, including their "Social Security numbers, job assignments, performance ratings and training information."[136] The second reported breach involved the theft of data on 19.7 million current, former, and prospective employees, and contractors who applied for a background investigation in 2000 or after using certain OPM forms.[137] This second breach also impacted the personal information of 1.8 million non-applicants; OPM notes that these non-applicants are primarily individuals married to or otherwise cohabitating with background investigation applicants.[138]

OPM confirmed the "[u]sernames and passwords that background investigation applicants used to fill out their background investigation forms were also stolen."[139] Notably, the two breaches revealed in June 2015 were not the first incidents targeting OPM databases containing such sensitive information.[140] In a previous 2014 breach of OPM, hackers purportedly targeted "files on tens of thousands of employees who [had] applied for top-secret security clearances."[141]

Reportedly, the hackers used compromised security credentials—those assigned to a KeyPoint Government Solutions employee, a federal background check contractor working on OPM systems—to exploit OPM's systems and

---

CONG. REC. D770 (daily ed. June 25, 2015); 114 CONG. REC. D762 (daily ed. June 24, 2015); *A Review of IT Spending and Data Security at OPM: Hearing Before the Subcomm. on Fin. Serv. & Gen. Gov't for Fiscal Year 2016, S. Comm. on Appropriations*, 114th Cong. 6 (2015), http://1.usa.gov/1pEmh7j (statement of Hon. Katherine Archuleta, Director of the Office of Personal Management); 114 CONG. REC. D715 (daily ed. June 16, 2015).

135 Press Release, House Comm. on Oversight & Gov't Reform, Fingerprints of Additional 4.5 Million Individuals Stolen in OPM Breach, Chaffetz Responds (Sept. 23, 2015), http://1.usa.gov/1OT6Xzp.

136 *Is the OPM Data Breach the Tip of the Iceberg?: Hearing Before the Subcomm. on Res., Tech. & Oversight, H.R. Comm. on Sci., Space & Tech.,* 114th Cong. 2 (July 8, 2015), http://1.usa.gov/1REyEHa; *see also* Nakashima I, *supra* note 5.

137 OPM - Steps to Protect Fed. Workers, *supra* note 19 (including the SF-85, SF-85P, and SF-86 forms and apply to applications for non-sensitive positions, public trust positions, and national security positions.).

138 *Id*.

139 *Id*.

140 *See* Michael S. Schmidt, David E. Sanger, & Nicole Perlroth, *Chinese Hackers Pursue Key Data on U.S. Workers,* N.Y. TIMES (July 9, 2014), http://nyti.ms/1XsquYS.

141 *Id*.

gain access. Officials do not believe the intruders are still in the system.[142] In the aftermath of the intrusions, Katherine Archuleta stepped down as the director of OPM amid several criticisms with how she managed the agency's response to the hack, but to many it was merely a passing of blame.[143] Beth Cobert, Deputy Director for Management and the U.S. Chief Performance Officer since October 2013, was appointed interim acting director for the agency following Archuleta's resignation[144] and President Obama has announced his intention to nominate her as the permanent replacement.[145] In addition, OPM's Electronic Questionnaires for Investigations Processing application, the "web-based automated system that was designed to facilitate the processing of standard investigative forms used when conducting background investigations," has been taken offline for "security enhancements."[146]

1. Why OPM?

To the typical civilian, OPM is better likened to the Human Resources Department of any business.[147] As such, the agency is responsible for the collection and storage of a substantial amount of confidential and sensitive personnel records for roughly 32 million past, current, and potential federal employees.[148] Given the nature of federal employment positions, OPM conducts "over two million background investigations yearly with over 650,000 conducted to sup-

---

142 *See*, *e.g.*, 114 CONG. REC. D715 (daily ed. June 16, 2015).

143 Sarah Wheaton & David Perera, *Archuleta's Out, but OPM's Problems Run Deep*, POLITICO (July 10, 2015, 12:45 PM), http://politi.co/1pMuLdk ("Criticism of Archuleta mounted last month after she deflected blame for the data breaches during a House Oversight and Government Reform Committee hearing in June, saying decades of neglecting government security systems was at fault.").

144 Evan Perez and Wesley Bruer, *OPM Director Katherine Archuleta steps down*, CNN (July 11, 2015 10:06 AM), http://cnn.it/1Tvmgee.

145 Press Release, White House, President Obama Announces His Intent to Nominate Beth Cobert as Director of the Office of Personnel Management (Nov. 10, 2015), http://1.usa.gov/1UVF0Hw.

146 *e-QIP Application Overview*, OFFICE OF PERSONNEL MGMT. (last visited Mar. 8, 2016), http://1.usa.gov/1SfvTfP.

147 Dominic Rushe, *OPM hack: China blamed for massive breach of US government data*, GUARDIAN (June 5, 2015 04:16 AM), http://bit.ly/1s5CeoH; Kaveh Waddell, *OPM Just Now Figured Out How Much Data It Owns*, ATLANTIC (NOV. 30, 2015), http://theatln.tc/1RlmUc5.

148 OFFICE OF PERSONNEL MGMT., CONGRESSIONAL BUDGET JUSTIFICATION PERFORMANCE BUDGET, FISCAL YEAR 2016, (2015), http://1.usa.gov/1SfU8dO ("As a proprietor of sensitive data—including personally identifiable information for 32 million federal employees and retirees - OPM has an obligation to maintain contemporary and robust cybersecurity controls. The infiltration of our network last year underscores the importance of these investments.").

port initial security clearance determinations…more than 95% of the Government total."[149]

As an applicant for security clearances, one must "complete a 127-page Standard Form-86 ("SF-86"), which contains all of their personal information, work history, family, associates, deviances, and proclivities."[150] "In the latter breach, 21.5 million SF-86 were successfully extracted by an unknown actor."[151] This amount of data collected and stored creates a treasure trove of federal data, including the most sensitive personal records of persons whom have worked in the Federal Government, as far as 1985.[152] Some have even likened the breach to stealing the "crown jewels" of federal information, because several million of the compromised records contain the identities and information of many covert federal operators.[153]

2. What Went Wrong at OPM?

Given the sensitive nature of the data that OPM collects and stores on it servers, it should come as no surprise that OPM on average receives "10 million confirmed intrusion attempts" targeting its network infrastructure each month.[154] While these intrusions are often unauthorized attempts that are more readily detectable under the current cybersecurity framework, the larger threat to the nation's cyberspace has increasingly come from authorized intrusions that result from compromised employee credentials and legitimate access to the network.[155] This threat has become so effective that even the DHS's newest systems designed to monitor and detect malicious threats have difficulty deci-

---

149 OFFICE OF PERSONNEL MGMT., FED. INVESTIGATIVE SERVS., ANNUAL REPORT TO STAKEHOLDERS: FISCAL YEAR 2014, at 22 (2014), http://1.usa.gov/1UQP7P4.

150 HANDING OVER THE KEYS TO THE CASTLE, *supra* note 47, at 3.

151 MOVING FORWARD, *supra* note 73, at 5.

152 Nakashima II, *supra* note 29.

> Stored in the system are massive amounts of data, including applicants' financial histories and investment records, children's and relatives' names, foreign trips taken and contacts with foreign nationals, past residences, and names of neighbors and close friends such as college roommates and co-workers. Employees log in using their Social Security numbers.

Id.

153 David Perera & Joseph Marks, *Newly Disclosed Hack Got 'Crown Jewels'*, POLITICO (June 12, 2015, 6:50 PM), http://politi.co/1pEu7xN ("'This is crown jewels material … a gold mine for a foreign intelligence service,' said Joel Brenner, a former NSA senior counsel.").

154 *OPM: Data Breach: Hearing Before the H. Comm. on Oversight & Gov't Reform,* 114th Cong. (June 16, 2015), http://1.usa.gov/1SfUvp1 (written statement of Katherine Archuleta, Former Director, Office of Personnel Mgmt.).

155 David M. Upton and Sadie Creese, *The Danger from Within*, HARV. BUS. REV. (Sept. 2014), http://bit.ly/1XsqOac.

phering what is legitimate and what is truly malicious when it is perpetrated by compromised credentials.[156] Since the OPM Breach, congressional inquiry and agency reports have suggested that, despite this threat, OPM possessed the necessary resources and were repeatedly put on notice of the potential security threat that their legacy systems posed to the data they maintain.[157]

In November 2013, actors breached OPM systems and extracted "manuals" relating to network assets and information about the internal infrastructure.[158] In August 2014, OPM's largest contractor tasked with providing background investigation services, USIS, disclosed a breach of its systems by Chinese hacker that lasted for over a year and compromised the information of approximately 27,000 DHS employees.[159] USIS filed for bankruptcy immediately following OPM's decision to rescind its contracts and delegated all background checks to KeyPoint.[160] In December 2014, KeyPoint disclosed a breach of its network, which had lasted at least 10 months and may have compromised the information of 48,439 federal workers.[161]

In OPM's 2014 audit, the Inspector General Michael Esser, provided a total of 29 recommendations covering a wide variety of IT security topics.[162] According to his own testimony during a July 2015 congressional hearing, "Only 3 of these 29 recommendations have been closed to date, and 9 of the open recommendations are long-standing issues that were rolled forward from prior year FISMA audits."[163] However, the three major vulnerabilities in OPM's

---

156 Aaron Boyd, *DHS cyber moving beyond signature-based protection*, FED. TIMES (March 23, 2016), 12:34 PM), http://bit.ly/22mupHO.

157 MICHAEL R. ESSER, U.S. OFFICE OF PERSONNEL MGMT., REPORT NO. 4A-CI-00-14-016, FINAL AUDIT REPORT: FEDERAL INFORMATION SECURITY MANAGEMENT ACT AUDIT FY2014, at 19-20 (2014), http://1.usa.gov/1TdetFv; *see also* Sean Gallagher, *"EPIC" fail—how OPM hackers tapped the mother lode of espionage data*, ARS TECHNICA (June 21, 2015, 10:30 PM), http://bit.ly/1WOCD8p; Dina Temple-Raston, *U.S. Officials Say Nearly 14 Million Affected In OPM Breach*, NPR (June 16, 2015, 6:22 AM), http://n.pr/1UOq8vL.

158 Evan Perez & Tom LoBianco, *U.S. Government Hacking Number Sparks Unusual Drama at Senate Briefing*, CNN (June 24, 2015, 4:57 PM), http://cnn.it/1ofze6s ("Asked if those manuals were akin to blueprints of OPM's computer systems, [OPM's CIO] Seymour answered, 'It would be fair to say that would give you enough information that you could learn about the platform, the infrastructure of our system, yes.'").

159 Kaveh Waddell and Stephanie Stamm, *A Timeline of Government Data Breaches*, NAT'L J. (July 6, 2015), http://bit.ly/1Ts9JxH.

160 *Id.*; INST. FOR CRITICAL INFRASTRUCTURE TECH., supra note 47, at 3.

161 Zach Noble, *OPM Contractors in the Crosshairs,* FCW (June 24, 2015), https://fcw.com/articles/2015/06/24/house-oversight-opm.aspx; Nick Wakeman, *Hackers hit OPM background investigations contractor,* WASH. TECH. (Dec. 18, 2014, 11:45 AM), http://bit.ly/1UVNcHz.

162 *See generally* ESSER, *supra* note 156, at 11-36.

163 *OPM Data Breach: Part II: Hearing Before the Subcomm. on Res. & Tech. in the H. Comm. on Sci., Space & Tech.*, 114th Cong. (July 8, 2015) (statement of Patrick E. McFarland, Inspector General, Office of Personnel Mgmt.).

Cyber Security Protocol contributed to the security incident, which includes: decentralized cybersecurity governance, outdated systems authorization, and non-compliant policies, procedures and technical controls.[164]

Without a centralized cybersecurity team responsible for overseeing all of OPM's cybersecurity efforts, OPM created many instances of non-compliance with FISMA requirements.[165] Primarily, OPM's Office of the Chief Information Officer ("OCIO"), is responsible for the agency's overall cybersecurity infrastructure and implementation of security controls.[166] However, such responsibilities have been subsequently found to have resided within individual program offices, leaving many important upgrade programs unimplemented, untested, and the department in much disagreement about the overarching cybersecurity strategy. Such deficiencies were well documented in all of the OIG's Audit Reports, dating back to 2007; however, the implementation of some new reporting structures within have contributed to better communication within the various program offices and the OCIO.[167]

The OIG found that OPM was not in compliance with several standards promulgated under 40 U.S.C. § 11331,[168] as is required by FISMA 2014, including in the areas of risk management, configuration management, incident response and reporting, continuous monitoring management, contractor systems, security capital planning, and contingency planning.[169] According to the OIG's Congressional testimony, "Not only was a large volume (11 out of 47 systems) of OPM's IT systems operating without a valid Authorization, but several of these systems are among the most critical and sensitive applications owned by the agency."[170] Even in the wake of the breach, the OIG instructed that OPM's Director strongly consider shutting down software systems that did not have a current and valid authorization.[171] In the audit report, however, the OIG noted OPM refused and instead stated it would work with information

---

164 Memorandum from Inspector General McFarland to Director Archuleta, *supra* note 32.

165 *See* ESSER, *supra* note 156, at 4-6.

166 Eric Yoder, *OPM officials hindering scrutiny of hacked computer systems, watchdog says*, WASH. POST (Aug. 6, 2015), http://wapo.st/1YT6Jss.

167 *OPM Data Breach: Part I: Hearing Before the S. Comm. on Homeland Sec. & Gov't Affs.,* 114th Cong. (June 25, 2015) [hereinafter *OPM Data Breach: Part I*] (statement of Patrick E. McFarland, Inspector General, U.S. Office of Personnel Mgmt.) ("OPM has implemented a team of Information System Security Officers (ISSO) that report to the OCIO and who have responsibility for managing security for the agency's various information systems.").

168 40 U.S.C. § 11331.

169 *Id.*

170 *OPM Data Breach: Part I, supra* note 167 (statement of Patrick E. McFarland, Inspector General, U.S. Office of Personnel Mgmt.).

171 Michael D. Maloney & Charles R. Lucy, *OPM Data Breach (cont'd): What We Know Now and What Questions Remain*, NAT'L L. REV. (July 20, 2015) http://bit.ly/1LSQrOP.

system security officers, both to ensure OPM systems maintain current authorizations and no interruptions to OPM's operations.[172]

While there is much to be said about the events that led to the failure of OPM's cybersecurity infrastructure and the failure of its managers to implement a centralized cybersecurity system, the events of the Breach have since led to the resignation of Katherine Archuleta and congressional calls for the removal of OPM's CIO, Donna Seymour.[173] Inquiries into the cybersecurity incident continue, but the public's interest in the agency's excuses has waned. OPM has announced that it will suspend some program systems and applications in order to update their authentication systems. Additionally, OPM has announced they would provide three years of credit monitoring services to those affected by the cybersecurity failure in order to show some attempt in restoring citizens' trust in the agency's responsibility of conducting federal background investigations.[174] While some have condemned the abysmal effort to bandage what is otherwise unrecoverable sensitive personal information, OPM continues to show a lack of remorse for this failure and it appears those who are most plausibly responsible for allowing the hack will retreat in peace.[175]

---

[172] MICHAEL R. ESSER, U.S. OFFICE OF PERSONNEL MGMT., REPORT NO. 4A-IS-00-14-017, FINAL AUDIT REPORT: AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S INVESTIGATIONS, TRACKING, ASSIGNING, AND EXPEDITING SYSTEM FY 2014, at 7-8 (2014), http://1.usa.gov/1ofBhYp.

[173] Julie Hirschfeld Davis, *Katherine Archuleta, Director of Personnel Agency, Resigns*, N.Y. TIMES (July 10, 2015), http://nyti.ms/1U7fL0G.

> [S]he felt new leadership was needed at the federal personnel agency to enable it to "move beyond the current challenges."…Her resignation marked a swift reversal but did little to calm the aftershocks of the disclosure this week of what appears to be the largest cybertheft affecting the federal government.

Id.; Letter from Rep. Jason Chaffetz to Hon. Beth Cobert, Director, Office of Personnel Mgmt. (July 22, 2015) ("I am deeply troubled Ms. Seymour remains at her post over a month after this request was made. My concerns about Ms. Seymour's ability to serve are amplified by a communication the Committee received from the Inspector General.").

[174] OPM - Steps to Protect Fed. Workers, *supra* note 19.

[175] Brian Krebs, *OPM (Mis)Spends $133M on Credit Monitoring*, KREBSONSECURITY (Sept. 2, 2015), http://bit.ly/1NHQz4D.

> The Office of Personnel Management (OPM) has awarded a $133 million contract to a private firm in an effort to provide credit monitoring services for three years to nearly 22 million people who had their Social Security numbers and other sensitive data stolen by cybercriminals. But perhaps the agency should be offering the option to pay for the cost that victims may incur in "freezing" their credit files, a much more effective way of preventing identity theft.

Id.

IV. OPM BREACH CLASS ACTIONS KEEP PILING UP

Amidst a flurry of bureaucratic banter, congressional inquiry, and administrative politicking, those affected by the colossal failure of the programs and systems they trusted to safe keep their sensitive personal information were quick to shoot back with a flood of class actions lawsuits citing a whole host of legal claims, with more bound to follow. As early as June 29, 2015, the American Federation of Government Employees ("AFGE"), together with the American Federation of Labor and Congress of Industrial Organizations ("AFL-CIO"), filed the largest class action against OPM, citing nearly 650,000 of its union members having been directly impacted by the breach.[176] Within a week, the National Treasury Employees Union ("NTEU"), which represents 150,000 employees across 31 federal agencies and departments, filed a suit directed at OPM's then-Director Katherine Archuleta accusing her of failing act properly in her capacity as an agency head and negligence with regard to protecting federal workers' data.[177] Since these cases several other smaller class actions have filed on by affected individuals, enjoining others affected by the breach.[178]

Each case shares a common thread of legal claims stemming from the Breach and commonly name OPM, Katherine Archuleta, Donna Seymour, and KeyPoint Government Solutions, the contractor alleged to have handled OPM's background checks and suffered a computer network breach in 2014, as defendants.[179] Generally, the complaints allege OPM had been on notice of cybersecurity deficiencies since 2007, compounding its failure to comply with the Privacy Act of 1974,[180] the Administrative Procedure Act,[181] FISMA and

---

176 Complaint at 8, Am. Fed. of Gov't Emp. et al. v. Office of Personnel Mgmt. et al., Case No. 1:15-cv-1015 (D.D.C. June 29, 2015), http://bit.ly/1UVQPgV.

177 Complaint at 19, Nat'l Treas. Emp. Union v. Archuleta, Case No. 15-3144 (N.D.Cal. July 8, 2015), http://bit.ly/25rCQ7w [hereinafter Complaint for Nat'l Treas. Emp. Union et al. v. Archuleta].

178 *See*, *e.g.*, Krippendorf v. United States, et al., Case No. 1:15-cv-01321 (D.D.C. Aug. 14, 2015), http://bit.ly/1SpzGK9; Woo v. Office of Personnel Mgmt. et al., Case No. 6:15-01220 (D.Kan. July 15, 2015); McGarry v. Office of Personnel Mgmt. et al., Case No. 1:15-cv-01705 (D.Col. Aug. 7, 2015); Hanagan v. Office of Personnel Mgmt. et al., Case No. 2:15-cv-06045 (C.D.Cal. Aug. 10, 2015).

179 Transfer Order at 2, *In re* U.S. Office of Personnel Mgmt. Data Sec. Breach Litig., MDL No. 2664 (J.P.M.L. Oct. 9, 2015) [hereinafter *In re* U.S. Office of Personnel Mgmt. Data Sec. Breach Litig.] ("Centralization will eliminate duplicative discovery, prevent inconsistent pretrial rulings on class certification and other issues, and conserve the resources of the parties, their counsel and the judiciary.").

180 5 U.S.C. § 552a.

> [R]equires federal agencies to establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity that could result in substantial harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained.

the so-called improvements within FISMA 2014;[182] even going so far as to claim common law negligence, and a violation of the Due Process Clause of the U.S. Constitution.[183]

A. National Treasury Employees Union v. Katherine Archuleta

Unique to the other class action suits brought against OPM in the wake of the breach, the NTEU cites Katherine Archuleta, OPM's former Director as the sole defendant on grounds she is to be held negligent to the extent of her capacity as the head of a federal agency.[184] By failing to heed the repeated warnings of OPM's OIG and otherwise failing to satisfy obligations imposed on her by statute and other appropriate authority, the complaint suggests Archuleta "manifested reckless indifference to its obligation to safeguard personal information provided by NTEU members with the assurance that it would be protected against unauthorized disclosure."[185] As such, the NTEU argues Director Archuleta violated NTEU members' constitutional right to informational privacy, including their right to Due Process under the Fifth Amendment.[186]

B. American Federation of Government Employees and AFL-CIO v. OPM, et. all

While the NTEU complaint targets Director Archuleta, the AFGE and AFL-CIO in the U.S. District Court for the District of Columbia jointly filed their complaint citing a whole host of procedural and administrative violations that extend beyond the former Director to include the agency as a whole and the third party contractors it utilized to develop its cybersecurity systems.[187] The AFGE stated that they "will not sit idly by while OPM fails to comply with the most basic requests for information or provide an adequate response. Even after this historic security breach, OPM has continued to use poor data security practices and inferior private-sector strategies to solve its security woes."[188]

Id.

181 Amanda Bronstad, *DOJ Wants Massive Government Data Breach Suits Consolidated*, NAT'L L. J. (Sept. 17, 2015), http://bit.ly/1TzE4Y6.

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

183 *See generally* U.S. CONST. amend. V.

184 Complaint for Nat'l Treas. Emp. Union et al. v. Archuleta, *supra* note 177, at 19.

185 *Id.*

186 *Id*.

187 *Id.*

188 Press Release, Am. Fed. of Gov't Emp., AFGE files Class Action Lawsuit against OPM Officials over Data Breach (June 29, 2015), http://bit.ly/1RvyZN7.

Most notably, the complaint cites violation of the Privacy Act of 1974[189] and the Administrative Procedure Act.[190]

C. Transfer and Consolidation

Despite the efforts of the affected individuals, the legal and procedural hurdles that such claims may face could impact their standing in the various districts where the complaints have been filed. Even now, the Department of Justice has already filed a Motion for Transfer of Actions with the U.S. Judicial Panel on Multidistrict Litigation ("JPML") in an effort to consolidate the complaints.[191]

On October 1st, the Panel heard arguments on authorization of transfer to the U.S. District Court for the District of Columbia.[192] Despite opposition to centralization from the NTEU[193], on October 9, 2015, the JPML ordered the transfer and centralization of the various claims to the District of Columbia given the common factual basis for the claims and requested relief.[194] While the order applies to the three cases that the Justice Department submitted, the Panel recognized that there are eleven other pending cases against OPM following the breach, that qualify also to be included in the centralization and transfer.[195] On March 14, 2016, counsel for the plaintiffs joined and submitted the amended consolidated complaint.[196] The newly amended complaint includes forty named plaintiffs against the defendants, which have been limited to the United States through OPM in its agency capacity and KeyPoint.[197]

V. IT'S TIME FOR A CHANGE: A PROPOSAL FOR A CYBERSECURITY REFORM SOLUTION

The U.S. cybersecurity infrastructure system must adapt to better manage

---

189 5 U.S.C. § 552(a).

190 *Id.* §§ 500-596.

191 *In re* U.S. Office of Personnel Mgmt. Data Sec. Breach Litig., *supra* note 179, at 2

192 *Id.*

193 Jody Godoy, *OPM Data Breach Suits Will Be Heard In DC, MDL Panel Says*, LAW360 (Oct. 13, 2015), http://bit.ly/1pT1opS ("The National Treasury Employees Union, which sued the OPM in July on behalf of its roughly 150,000 federal employee members, had asked the panel to exempt it from consolidation, arguing that the suit was not a class action like many of the others and that it had raised different legal claims.").

194 *In re* U.S. Office of Personnel Mgmt. Data Sec. Breach Litig., *supra* note 179, at 2.

195 Godoy, *supra* note 193 (quoting the panel order) ("Centralization will eliminate duplicative discovery, prevent inconsistent pretrial rulings on class certification and other issues, and conserve the resources of the parties, their counsel and the judiciary….").

196 *In Re:* U.S. Office of Personnel Mgmt. Data Sec. Breach Litig., Case 1:15-mc-01394-ABJ (D.D.C. March, 3, 2016).

197 *Id.*

federal data. The current state of federal law, amidst the rise of cyber threats, still lags behind the rapid development of technology; and recent efforts to enact cybersecurity legislation have failed. A complete overhaul is the only way to achieve a more secure data management infrastructure. While this is easier said than done, it is necessary to entertain all possible solutions in order to effectively implement meaningful reform that will better secure federal cybersecurity infrastructure.

Essentially, the current framework must be upended. A centralized cybersecurity framework that delegates to DHS regulatory, policing, and enforcement power to more thoroughly account for the nature of cybersecurity threats and the impact that breaches pose to national security. In addition, any cybersecurity legislation must enhance oversight of federal agencies and government contractors providing information technology and cybersecurity services to the government.[198] This would extend liability on them, similar to the liability that has been imposed on private companies to protect civilian data.[199] Furthermore, given the sensitive nature of security clearances for the federal workforce and the Federal Government's interest in protecting national security it is argued here DHS should be granted the authority to complete the federal background check process for potential future federal employees. While this grant would centralize the process of background checks for the majority of federal employees, defense and intelligence agencies such the DOD and the Central Intelligence Agency should retain their authority to conduct their own background checks.

Similar to the proposed legislation under the Federal Information Security Management Reform Act of 2015 currently pending before the 114th Congress, DHS must be tasked with "conducting targeted risk assessments and operational evaluations."[200] The current framework is inadequate because DHS has limited ability to shield agency networks with its highly invested cybersecurity monitoring platform, EINSTEIN.[201] DHS can only enter an agency's network with EINSTEIN if the agency asks for help.[202] Under the proposed law, DHS could run intrusion detection and prevention technology on all agen-

---

198 GAO-15-714, *supra* note 46, at 45.

199 Ellen Nakashima & Katie Zezima, *Obama to Propose Legislation to Protect Firms that Share Cyberthreat Data*, WASH. POST (Jan. 12, 2015), http://wapo.st/1ofGIGH.

200 Federal Information Security Management Reform Act of 2015 § 2, H.R. 3402, 114th Cong. (2015).

201 *See EINSTEIN*, DEP'T OF HOMELAND SEC., http://1.usa.gov/1PzBWdk (last visited Mar. 4, 2016).

202 *See generally* Model Agreement Relating to the Deployment of EINSTEIN Cybersecurity Capabilities, Department of Homeland Security, Office of Cybersecurity and Communications, http://1.usa.gov/1RJ3QLy.

cy systems. Given the existing investment in cybersecurity infrastructure within federal agencies, congressional legislation like the FISMA Reform Act of 2015 must grant DHS centralized authority to immediately deploy the EINSTEIN platform in its full monitoring capacity within every federal agency. Together with binding authority, it is recommended that DHS be given the authority to improve security incident response activities by suspending agency cybersecurity programs if programs do not meet statutorily imposed auditing requirements. In the interest of national security, DHS must be given the authority to take control of agency networks during cyber-emergencies and clearly define what a cyber-emergency might constitute.

The cornerstone of any cybersecurity legislative reform is the inclusion of administrative and judicial mechanisms for extending liability on those internally responsible for allowing federal systems to fail, the ability to aggressively pursue cyber criminals, and initiate countervailing measures where foreign nation-states have engaged in unwarranted government espionage. In many instances, the government enjoys sovereign immunity, meaning it cannot face civil suits or prosecution over most subjects.[203] Under the Federal Torts Claims Act,[204] individuals can sue federal employees for negligence within the scope of their jobs.[205] This negligence can extend to "loss of property, or personal injury or death arising or resulting from the negligent or wrongful act or omission of any employee of the Government."[206] Under the current standard, courts have been hesitant to extend property protections to personal data; however, redefining personal information and data stored as personal property would offer a more comprehensive legal framework for courts to apply in the event of data breaches.[207]

The more paramount concern, in addition to domestic security efforts, lies in the ability of the United States to combat cyber-warfare abroad. As attacks become more sophisticated, particularly in foreign regimes that promote government and industrial espionage, the United States must remain committed to engaging and setting the global standards for cybersecurity. However, when domestic policy is fragmented, the nation's ability to hold the International Community to such policies is severely diminished. Evidence that progress is being made in this area has come following an official state visit from China's President Xi Jinping.[208] On September 25, 2015, President Obama and Presi-

---

[203] *Sovereign Immunity*, LEGAL INFO. INST., http://bit.ly/1Rn3UP2 (last visited Mar. 6, 2016).

[204] *See generally* Federal Tort Claims Act, 28 U.S.C. §§ 1346(b), 2671-2680 (2012).

[205] *See* 28 U.S.C. § 2679(b)(1) (2012).

[206] *Id*.

[207] Cory Bennett, *OPM Letter Distances Agency from Legal Liability Over Hack*, THE HILL (June 18, 2015, 3:18 PM), http://bit.ly/1RkC0Dp.

[208] Dave Boyer, *Obama to Host China's Xi Jinping Despite Cyberattacks*, WASH. TIMES

dent Xi announced an agreement between the United States and China to establish an open dialogue on combatting cybercrimes.[209]

As part of the agreement, each commits to investigate cybercrimes, collect electronic evidence, and mitigate malicious cyber activity emanating from its territory, and to provide timely responses to requests for information and assistance concerning those activities.[210] Furthermore, the U.S. and China will establish a high-level joint dialogue mechanism on fighting cybercrime and related issues.[211] Perhaps most importantly, these nations committed that "neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[212]

Only time will tell whether these countries will live up to their commitments. According to the agreement, the Secretary of Homeland Security and the Attorney General will co-chair the dialogue on the U.S. side, which signifies an effort to centralize the role DHS will play in future direction of the American cybersecurity policy, and ensure that China fulfills its commitments to advance progress made thus far.[213] To be sure, the agreed commitments do not resolve all challenges between the U.S. and China or other nation-states on cyber issues.[214] However, according to DHS Secretary Jeh Johnson, it does "represent a step forward in U.S. efforts to address one of the sharpest areas of disagreement in the U.S.-China bilateral relationship."[215] In the wake of the OPM Breach, the U.S. seemingly is working to address its own shortcomings on cybersecurity and meet the commitments of this new agreement.[216]

(June 10, 2015) http://bit.ly/1VfYU10; *see also* David Nakamura, *White House Formally Announces Chinese President Xi Jinping's First State Visit on Sept. 25*, WASH. POST (Sept. 15, 2015), http://bit.ly/1VfYU10.

209 Press Release, Office of the Press Secretary, White House, FACT SHEET: President Xi Jinping's State Visit to the United States (Sept. 25, 2015), http://1.usa.gov/1SlDdt9.

210 *Id.* ("Both sides also agreed to provide updates on the status and results of those investigations and to take appropriate action.").

211 *Id*.

212 *Id*.

213 Ellen Nakashima & Steven Mufson, *U.S., China Vow Not to Engage in Economic Cyberespionage*, WASH. POST. (Sept. 25, 2015), http://wapo.st/1RrUG2N.

214 Press Release, Dep't of Justice, Joint Statement by Attorney General Loretta E. Lynch and Secretary of Homeland Security Jeh Johnson (Sept. 25, 2015), http://1.usa.gov/1Rz340u.

215 Jeh C. Johnson, Secretary of Homeland Security, Remarks at Cybercon 2015 (Nov. 9, 2015), http://1.usa.gov/1pEFTrW.

216 Tim Starks, *Taking Stock of Obama's Cyber Record*, POLITICO (Jan. 7, 2016, 1:00 AM), http://politi.co/1SbtK4S (quoting President Barack Obama) ("America's economic prosperity in the 21st century will depend on cybersecurity.").

CONCLUSION

The danger posed by the ever-growing threat of cyber-attacks against the nation is heightened by the revelation of the weaknesses and failures in the Federal Government's approach to cybersecurity despite having the budget to do so. While recent government initiatives have tried to combat the issue, it is important to note that no single technology or set of practices is sufficient to protect against all potential threats. A comprehensive and centralized strategy is required that includes well-trained personnel, effective and consistently applied processes, and appropriately implemented technologies. While agencies have elements of this strategy in place, more must be done to fully implement it and to remove existing weaknesses. Following the OPM Breach, OPM must be mandated to implement GAO and its Inspector General recommendations that will strengthen the agency's ability to protect their systems and information, reducing the risk of another potentially devastating cyber-attack.