OPM DATA BREACH CASE STUDY: MITIGATING PERSONNEL CYBERSECURITY RISK

ALAN WEHBÉ*

I. INTRODUCTION

In June 2016, I received a series of text messages from someone using a phone number that I did not recognize purporting to be an old acquaintance. I responded, trying to figure out who this stranger was, to no avail. In October, I again received a series of text messages from another person using a phone number I did not recognize, again purporting to be an acquaintance, but this time the other party was more insistent. Disturbingly, in trying to convince me

* Operations Attorney Advisor in the United States Department of Justice, National Security Division's Office of Intelligence and Judge Advocate (Major) in the United States Army Reserves, Judge Advocate General's Corps. Mr. Wehbé holds a M.A. in Education (2013) from Michigan State University; a J.D. (2005) from Villanova Law School; a M.B.A. (2005) from Villanova Business School; and a B.A. (2001) from Boston College. The opinions and conclusions expressed herein are solely those of the author. They do not necessarily reflect the views of the Attorney General of the United States, the United States Department of Justice, the Judge Advocate General of the United States Army, the Department of the Army, or any other government agency.

that "she" knew who I was, this second person was more aggressive in attempting to elicit personal facts about me. Something just did not feel right. How could a stranger have so much information about me? To this day I am convinced that it was a targeted attempt to exploit me[1] through some form of phishing[2] or similar act by some malign actor, whether foreign intelligence or simply criminal.

In spring 2015, it came to light that the U.S. Government's Office of Personnel Management (OPM) was the victim of a cyber-attack that resulted in the loss of a great deal of data.[3] As news of the so-called "data breach"[4] unfolded, countless news sources revealed an increasingly disturbing sequence of events in which data systems were breached and information regarding the breach was not reported in a timely fashion. The scope of the incident continued to grow in magnitude and is now also the subject of a federal lawsuit.[5] It further resulted

---

[1] A possible explanation for the level of information this person had was that they possessed my Standard Form 86, a document used to collect background information to conduct a background investigation for national security positions. *See*, OFFICE OF PERS. MGMT., QUESTIONNAIRE FOR NATIONAL SECURITY POSITIONS, STANDARD FORM 86, OMB FORM NO. 3206 0005 (Dec. 2010).

[2] "Phishing refers to the process where a targeted individual is contacted by email or telephone by someone posing as a legitimate institution to lure the individual into providing sensitive information such as banking information, credit card details, and passwords." *What is Phishing?*, PHISHING.ORG, http://www.phishing.org (last visited Nov. 11, 2015); *see also* Jennifer Lynch, *Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks*, 20 BERKELEY TECH. L.J. 259, 259 n. 2 (2005) ("The word 'phishing' comes from an analogy to fishing; the e-mail is bait used to lure in 'fish' from the 'sea' of Internet users. The 'f' is changed to 'ph' in keeping with computer hacking tradition." (citation omitted)).

[3] *See* STAFF OF H. COMM. ON OVERSIGHT AND GOV'T REFORM, 114TH CONG., THE OPM DATA BREACH: HOW THE GOVERNMENT JEOPARDIZED OUR NATIONAL SECURITY FOR MORE THAN A GENERATION 5–13 (Comm. Print 2016) (delineating the timeline revealed by the Committee Majority Staff's investigation) [hereinafter COMM. REPORT ON THE OPM DATA BREACH] *available at* https://oversight. house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf; Mike Levin, *OPM Hack Far Deeper Than Publicly Acknowledged, Went Undetected for More Than a Year, Sources Say*, ABCNEWS.COM (June 11, 2015, 4:59 PM), http://abcnews.go.com/Politics/opm-hack-deeper-publicly-acknowledged-undetected-year-sources/story?id=31689059 (explaining OPM's decision to inform four million government employees that their data may have been compromised).

[4] *See, e.g.*, Jes Alexander, *Anatomy of a Data Breach—What Cyber Policies Should Cover*, 13 J. TEX. INS. L. 5 (2015) (discussing implications of data breaches on private entities); Thad A. Davis et al., *The Data Security Governance Conundrum: Practical Solutions and Best Practices for the Boardroom and the C-Suite*, 2015 COLUM. BUS. L. REV. 613 (2015) (discussing corporate implications and government regulatory issues related to data breaches); Abraham Shaw, *Data Breach: From Notification to Prevention Using PCI DSS*, 43 COLUM. J.L. & SOC. PROBS. 517 (2010) (discussing data breaches generally).

[5] *See* Complaint at 2, Am. Fed'n of Gov't Emps. v. U.S. Office of Pers. Mgmt., No. 1:15-

in the federal government committing to spend "$330 million on anti-fraud protections for the 21.5 million victims . . . ."[6]

This event highlights several points for the federal government, the federal employee, and the American public writ large. First, it reminds us that the threat of cyber attacks,[7] hacks,[8] and similar events are ever-present.[9] Second, uniform requirements do not appear to be in place to report or notify the public, or appropriate officials when such events occur.[10] Third, it shows that the deficiency in training and awareness procedures and reporting processes currently in place fail to sufficiently mitigate these threats.[11] With the increasing threat of data breaches and other cybersecurity incidents, the federal government has

---

cv-1015, 2015 WL 4039005 (D.D.C. June 29, 2015) (federal employee association suing federal government for various damages resulting from data breach); *see also* Levin, *supra* note 3 (discussing the fact that OPM hack was likely "more problematic than publicly acknowledged").

[6] Aliya Sternstein, *Lawmakers Want National Security Damage Assessment on OPM Hack*, NEXTGOV.COM (Dec. 2, 2015), http://m.nextgov.com/cybersecurity/2015/12/lawmakers-want-national-security-damage-assessment-opm-hack/124108/?oref=ng-HPtopstory.

[7] *See generally* Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CAL. L. REV. 817, 822–39 (2012) (defining and discussing cyber-attacks).

[8] *See generally* Mary M. Calkins, *They Shoot Trojan Horses, Don't They? An Economic Analysis of Anti-Hacking Regulatory Models*, 89 GEO. L.J. 171 (2000) (defining and discussing hacking).

[9] *See* Eric G. Orlinsky et al., *Cybersecurity: A Legal Perspective*, 47 MD. B.J. 32 (2014) (discussing persistent and inevitable nature of cyber threat); Peter Margulies, *DOJ's "All-Tools" Approach to Cyber and National Security*, LAWFARE (Oct. 20, 2015, 7:07 AM), https://www.lawfareblog.com/dojs-all-tools-approach-cyber-and-national-security (discussing new approaches to cybersecurity, such as law enforcement, diplomacy, and use of force); *see, e.g.*, Susanna Bagdasarova, *Brave New World: Challenges in International Cybersecurity Strategy and the Need for Centralized Governance*, 119 PENN ST. L. REV. 1005 (2015) (discussing current state of international cybersecurity law and regulation and proposing centralized approach); Geoffrey S. Corn, *Averting the Inherent Dangers of "Going Dark": Why Congress Must Require a Locked Front Door to Encrypted Data*, 72 WASH. & LEE L. REV. 1433 (2015) (examining the tension between government access, encryption, and Fourth Amendment privacy concerns); Melanie J. Teplinsky, *Fiddling on the Roof: Recent Developments in Cybersecurity*, 2 AM. U. BUS. L. REV. 225 (2013) (examining the implications of the increasing cybersecurity threat on the corporate world).

[10] *See, e.g.*, Brandon Faulkner, *Hacking Into Data Breach Notification Laws*, 59 FLA. L. REV. 1097 (2007) (discussing motivation for private entities not to report data breaches); Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 932–44 (2007) (discussing requirements for notification of data security breaches in private sector); Jacqueline May Tom, *A Simple Compromise: The Need for a Federal Data Breach Notification Law*, 84 ST. JOHN'S L. REV. 1569 (2010) (arguing for a federal law regarding reporting and notification of data breaches).

[11] *See* Brian B. Kelly, *Investing in a Centralized Cybersecurity Infrastructure: Why "Hacktivism" Can and Should Influence Cybersecurity Reform*, 92 B.U. L. REV. 1663,

to improve its protection of the cybersecurity workforce[12] and in turn national security.[13] This paper will propose to improve the cybersecurity awareness of the federal workforce by implementing meaningful and effective cybersecurity awareness training and education, as well as delineating strict cybersecurity incident and data breach reporting guidelines to hold accountable those officials who attempt to contain bad news at their level or within their agency.[14]

This paper will examine the issues discussed above, analyze the gaps in current and proposed law[15] and policy related to them. Additionally, this study will recommend ways to fill the gaps and mitigate the risks in the context of personnel training and education, specifically by implementing certain laws and policies that will address the most readily mitigated threats of an ill-trained and ill-informed population[16] susceptible to financial and other exploitation.[17] This paper will, in part, attempt to redirect some of the attention focused on preven-

---

1695-96 (2012) (discussing federal proposals and efforts to recruit a cyber-aware workforce).

[12] "[T]he term 'Cybersecurity Category' means a position's or incumbent's primary work function involv[es] cybersecurity . . . ." Cybersecurity Workforce Assessment Act, Pub. L. No. 113-246, § 2, 128 Stat. 2880 (2014). Given the ambiguity of that definition and the purpose of this paper in seeking to protect the federal workforce generally, the terms "cybersecurity workforce" and "federal workforce" are used as functionally interchangeable.

[13] *See generally* COMM. REPORT ON THE OPM DATA BREACH, *supra* note 3, at v–x (executive summary discussing how OPM Data Breach presents a generational national security threat); Deborah Norris Rodin, *The Cybersecurity Partnership: A Proposal for Cyberthreat Information Sharing Between Contractors and the Federal Government*, 44 PUB. CONT. L.J. 505, 507-13 (2015) (discussing current cyberthreat to critical infrastructure and regulatory efforts to enhance cybersecurity).

[14] *See* Scott J. Shackelford et al., *Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT'L L.J. 305 (2015) (discussing the haphazard nature of regulatory enforcement in the context of cybersecurity data breaches).

[15] *See, e.g.*, Cybersecurity Information Sharing Act of 2015, 6 U.S.C.A. § 1501 (Westlaw through Pub. L. No. 114-219); Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2259 (2002); Clinger-Cohen Act of 1996, Pub. L. No. 104-106, 110 Stat. 679 (1996); *see also* Rodin, *supra* note 13, at 507–13; Mitchell S. Kominsky, *The Current Landscape of Cybersecurity Policy: Legislative Issues in the 113th Congress*, HARV. L. SCH. NAT'L SEC. J: ONLINE CONTENT (Feb. 6, 2014, 5:36 PM), http://harvardnsj.org/2014/02/the-current-landscape-of-cybersecurity-policy-legislative-issues-in-the-113th-congress (reviewing 113th Congress's efforts at cybersecurity law).

[16] *See* Noah G. Susskind, *Cybersecurity Compliance and Risk Management Strategies: What Directors, Officers, and Managers Need to Know*, 11 N.Y.U. J.L. & Bus. 573 (2015) (discussing corporate ignorance of cybersecurity practices).

[17] An example of such poor cybersecurity practices can be seen in nearly annual articles recounting the most common passwords used online. *See, e.g.*, Brett Molina, *Most Common Password in 2014: '123456,'* USA TODAY (Jan. 21, 2015, 8:37 AM), http://www.usatoday.com/story/tech/2015/01/20/worst-passwords/ 22056847; Chenda Ngak, *The 25 Most Com-*

tion of security breaches to mitigation by informing potential victims of such breaches. This paper is not intended to minimize the risk of breaches, but rather acknowledge that they will occur and propose a method of risk management that should be included in a broader cybersecurity strategy. Part I will review the information publicly available on the OPM Breach to include an analysis of the time frame from incident to reporting. Part II will review current law related to training government or contracted employees with regard to cybersecurity and cybersecurity incident reporting. Part III will identify key gaps in the current law related to cybersecurity and cybersecurity incident reporting. Part IV will make recommendations to fill the gaps identified in part III to mitigate the risks discussed.

II. THE OPM BREACH

Cybersecurity risk, as this paper will briefly survey, is endemic.[18] There is always another risk around the corner, always another hack or breach.[19] In fact, the breach suffered by the U.S. Office of Personnel Management (OPM), which is the focal point of this paper, actually may have consisted of four individual breaches, resulting in the well-publicized theft of personal information, fingerprint information, and other data.[20] Yet, reports indicate that key OPM officials were unaware of the breach until April 15, 2015.[21] There are accounts of various failures associated with each event, including possible signs of trouble or

---

mon Passwords of 2013, CBS NEWS (Jan. 21, 2014, 11:14 AM), http://www.cbsnews.com/news/the-25-most-common-passwords-of-2013; *see also* Lynch, *supra* note 2.

[18] *See* sources cited *supra* note 10 and accompanying text; *see also* Jeff Goldman, *Industry Experts Predict the Top Cyber Security Trends for 2016*, ESECURITY PLANET (Dec. 2, 2015), http://www.esecurityplanet.com/network-security/industry-experts-predict-the-top-cyber-security-trends-for-2016.html (describing trends in cybersecurity anticipated for 2016).

[19] *See* Goldman, *supra* note 18.

[20] *See* COMM. REPORT ON THE OPM DATA BREACH, *supra* note 3, at v–x (executive summary discussing how OPM Data Breach presents a generational national security threat); Christian Davenport, *KeyPoint Network Breach Could Affect Thousands of Federal Workers*, WASH. POST (Dec. 18, 2014), https://www.washingtonpost.com/business/economy/keypoint-suffers-network-breach-thousands-of-fed-workers-could-be-affected/2014/12/18/e6c7146c-86e1-11e4-a702-fa31ff4ae98e_story.html (describing fallout from the hacking of two separate federal background check contractors); Christian Davenport, *USIS Contracts for Background Security Checks Won't be Renewed,* WASH. POST (Sept. 9, 2014), https://www.washingtonpost.com/business/economy/opm-to-end-usis-contracts-for-background-security-checks/2014/09/09/4fcd490a-3880-11e4-9c9f-ebb47272e40e_story.html (detailing OPM's decision to stop using USIS for background checks following a cyberattack).

[21] *See* OFF. OF PERS. MGMT, NEWS RELEASE: OPM TO NOTIFY EMPLOYEES OF CYBERSECURITY INCIDENT (June 4, 2015) [hereinafter OFF. PERS. MGMT, NEWS RELEASE], https://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident/ ("[I]n April 2015, OPM detected a cyber-intrusion affecting its information technology (IT) systems and data."); Sean Lyngaas, *Exclusive: The OPM Breach Details You Haven't Seen*,

warnings ignored, failures or delays in reporting, and other issues that may have contributed to the depth of harm created by the breaches.[22] There were two prior breaches of government contractors leading up to the OPM breach: one at the United States Investigation Services (USIS) and the next at KeyPoint Government Solutions.[23] According to reports, the USIS breach occurred in March 2014 and was attributed to Chinese hackers, but was not immediately made public because officials did not believe any personally identifiable information was compromised or stolen.[24] News of that intrusion appears to have first been made public by the New York Times in July 2014.[25]

The Director of National Intelligence, James Clapper, suggested that China was to blame for the OPM breach.[26] Chinese authorities later arrested "a handful of hackers it says were connected to the breach of Office of Personnel Management's database," though "U.S. officials say they appear to have been carried out in an effort to lessen tensions with Washington."[27] While noteworthy, this paper will not address the problem of attribution of such attacks.[28]

FCW.COM (Aug. 21, 2015), https://fcw.com/articles/2015 /08/21/opm-breach-timeline.aspx (providing an in-depth timeline showing officials learning of the hack on April 15, 2015).

[22] *See* COMM. REPORT ON THE OPM DATA BREACH, *supra* note 3, at v–x (executive summary discussing scope of harm created by breach); *See* Complaint at 2, Am. Fed'n of Gov't Emps. v. U.S. Office of Pers. Mgmt., No. 1:15-cv-1015, 2015 WL 4039005 (D.D.C. filed June 29, 2015) (federal employee lawsuit alleging multiple deficiencies in OPM cybersecurity protocols).

[23] *See* sources cited *supra* note 20 and accompanying text.

[24] *See* David Bisson, *The OPM Breach: Timeline of a Hack*, TRIPWIRE.COM (July 10, 2015, 9:00 AM), http://www.tripwire.com/state-of-security/security-data-protection/cybersecurity/the-opm-breach-timeline-of-a-hack (providing a timeline which shows Chinese hackers infiltrating OPM computer systems in March, 2015); Michael S. Schmidt et al., *Chinese Hackers Pursue Key Data on U.S. Workers,* N.Y. TIMES (July 9, 2014), *available at* http://www.nytimes.com/2014/07/10/world/asia/chinese-hackers-pursue-key-data-on-us-workers.html?action=click&contentCollection=U.S.&module=RelatedCoverage&region=Marginalia&pgtype=article&_r=1 (quoting senior officials on the loss of PII and attributing the attack to Chinese hackers).

[25] *See* Schmidt et al., *supra* note 24.

[26] Damian Paletta, *U.S. Intelligence Chief James Clapper Suggests China Behind OPM Breach*, WALL ST. J. (June 25, 2015), *available at* http://www.wsj.com/articles/SB10007111583511843695404581069863170899504.

[27] Ellen Nakashima, *Chinese Government Has Arrested Hackers it Says Breached OPM Database*, WASH. POST (Dec. 2, 2015), https://www.washingtonpost.com/world/national-security/chinese-government-has-arrested-hackers-suspected-of-breaching-opm-database/2015/12/02/0295b918-990c-11e5-8917-653b65c809eb_story.html; *see* Roberto Baldwin, *China Says OPM Breach Was the Work of Criminal Hackers*, ENGADGET (Dec. 2, 2015), http://www.engadget.com/2015/12/02/china-opm-hack-blame.

[28] *See* Major Erik M. Mudrinich, *Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem*, 68 A.F. L. REV. 167 (2012) (describing the importance of attribution in U.S. cyber strategy); *see also*, Shane McGee et al.,

A. *USIS Breach*

The USIS breach was discovered several months before it was publicly reported.[29] In fact, the Chief Information Officer (CIO) of USIS testified that the company discovered and reported the breach to the OPM in June 2014.[30] Nonetheless, the USIS breach was not publicly reported until August 2014.[31] USIS reportedly believed it suffered a "state-sponsored attack."[32] The USIS CIO further noted before the House Committee on Government Oversight and Reform that, despite discovering the attack in June, USIS was not able to block and contain the attacker until July.[33] At the time of the breach, USIS was the "largest provider of background investigations for the federal government."[34] To give an idea of the scope of USIS's responsibilities at the time of the breach, it was believed that the attack compromised more than 25,000 background investigation files.[35]

B. *KeyPoint Breach*

KeyPoint Government Solutions ("KeyPoint") was awarded an indefinite quantity/ indefinite duration ("IDIQ")[36] contract in 2004 to provide background investigations for the OPM.[37] By February 2014, KeyPoint was performing

---

Adequate Attribution: A Framework for Developing a National Policy for Private Sector Use of Active Defense, 8 J. BUS. & TECH. L. 1, 4–6 (2013) (discussing the difficulty of attribution of cyber attacks).

[29] *See* COMM. REPORT ON THE OPM DATA BREACH, *supra* note 3, at 5–7 (outlining several key events where OPM officials were notified or aware of the data breach as early as March 20, 2014); *OPM Data Breach: Part II: Hearing Before the H. Comm. on Oversight and Gov't Reform*, 114th Cong. 1–2, (2015) (statement of Robert W. Giannetta, Sr., Chief Information Officer, US Investigations Services, LLC) [hereinafter Hearing] (stating that USIS "self-detected a cyber-attack" in June, 2014); Ellen Nakashima, *DHS Contractor Suffers Major Computer Breach, Officials Say*, WASH. POST (Aug. 6, 2014), https://www.washingtonpost.com/world/national-security/dhs-contractor-suffers-major-computer-breach-officials-say/2014/08/06/8ed131b4-1d89-11e4-ae54-0cfe1f974f8a_story.html (breaking the story of the USIS hack in August).

[30] *Id.*

[31] *See* Nakashima, *supra* note 29.

[32] *Id.*

[33] *See* Hearing, *supra* note 29.

[34] Nakashima, *supra*, note 29.

[35] Scott Neuman, *Government to Drop Background Check Firm USIS*, NPR (Sept. 10, 2014, 10:30 AM), http://www.npr.org/sections/thetwo-way/2014/09/10/347360843/ government-to-drop-background-check-firm-usis.

[36] *See, e.g.*, Markow W. Kipa et al., *Conquering Uncertainty in an Indefinite World: A Survey of Disputes Arising Under IDIQ Contracts*, 37 PUB. CONT. L.J. 415, 417–20 (2008) (explaining the basic features of IDIQ contracts).

[37] *DC Navy Yard Shooting: Fixing the Security Clearance Process: Hearing Before the H. Comm. on Oversight & Gov't Reform*, 113th Cong. 28 (2014) (statement of Susan A. Ordakowski, Vice President, Contracts and Compliance, KeyPoint Gov't Solutions).

"approximately 25 percent of the fieldwork conducted by contractors for OPM's background investigations."[38] KeyPoint publicly reported its breach in December 2014, but it appears that there was evidence of the breach as early as September.[39] Reports conflict on whether the OPM breach had already begun prior to the KeyPoint breach, or whether the KeyPoint breach was the foothold upon which the OPM breaches were executed.[40] KeyPoint's CEO testified that despite the breach, "after an extensive analysis of this incursion, we found no evidence of the exfiltration of sensitive personal data."[41]

C. *OPM Breach I*

In June 2015 the Office of Personnel Management[42] (OPM) reported, "the background investigation records of millions of current, former and prospective federal employees and contractors had been stolen in a cyber intrusion that started in early 2014."[43] Initial reports indicated that the intrusion had gone unnoticed for over a year, after the intruders created a "backdoor for exfiltration" of data with stolen credentials in May 2014.[44] Disturbingly, while investigating the initial breach, investigators discovered a second breach of the OPM networks.[45]

---

[38] *Id.*

[39] *See* Hearing, *supra* note 29 (statement of Eric Hess, Chief Exec. Officer and President, KeyPoint Gov't Solutions); Davenport, *supra* note 20.

[40] *See* Hearing, *supra* note 29 (statement of Eric Hess, Chief Exec. Officer and President, KeyPoint Gov't Solutions) (claiming there is no evidence suggesting that KeyPoint was responsible for the OPM breach); Aaron Boyd, *Contractor Breach Gave Hackers Keys to OPM Data*, FED. TIMES (June 23, 2015), http://www.federaltimes.com/story/government/omr/opm-cyber-report/2015/06/23/keypoint-usis-opm-breach/28977277 ("Keypoint . . . gave hackers the credentials needed to access sensitive employee data held by the [OPM]."); *see also* Davenport, *supra* note 20; Evan Perez & Shimon Prokupecz, *First on CNN: U.S. Data Hack May be 4 Times Larger Than the Government Originally Said*, CNN (June 23, 2015), http://www.cnn.com/2015/06/22/politics/opm-hack-18-milliion.

[41] *See* Hearing, *supra* note 29 (statement of Eric Hess, Chief Exec. Officer and President, KeyPoint Gov't Solutions).

[42] The Office of Personnel Management (OPM) is the successor of the Civil Service Commission, established by the Civil Service Act, ch. 27, § 1, 22 Stat. 403 (1883). The Civil Service Reform Act of 1978 eliminated the Civil Service Commission and distributed its functions into three new organizations including the Office of Personnel Management. Civil Service Reform Act of 1978, Pub. L. No. 95–454, 92 Stat. 1111 (1978). The OPM was generally charged with being responsible for personnel management of the civil service of the Government. § 1104, 92 Stat. at 1120.

[43] James Eng, *OPM Hack: Government Finally Starts Notifying 21.5 Million Victims*, NBC NEWS (Oct. 1, 2015), http://www.nbcnews.com/tech/security/opm-hack-government-finally-starts-notifying-21-5-million-victims-n437126; *See* OFF. PERS. MGMT, NEWS RELEASE, *supra* note 21.

[44] Levin, *supra* note 3; Lyngaas, *supra* note 21.

[45] Hearing, *supra* note 29 (statement of Katherine Archuleta, Director, Off. Pers. Mgmt.);

D. *OPM Breach II*

The second OPM breach was discovered in late May 2015, while OPM was investigating the initial breach with assistance from the Federal Bureau of Investigation ("FBI") and the Department of Homeland Security ("DHS").[46] The second breach led the OPM's Director, Katherine Archuleta, to testify that there "was a high degree of confidence that OPM systems related to background investigations of current, former, and prospective Federal government employees, and those for whom a federal background investigation was conducted, may have been compromised."[47] These events collectively underscore the fact that cybersecurity incidents and data breaches will happen.

E. *Reporting Delays*

There are two disturbing features of the OPM Breach that created an additional risk to the people exposed to the breach: failures in reporting and delays in notifications. The first sign of a problem appears to have occurred in June 2014, when USIS discovered and reported the first intrusion to the OPM.[48] Yet, OPM did not fully publicly release this information until June 2015, stating that "OPM will send notifications to approximately 4 million individuals" who may have been impacted — employee notifications that were ongoing as late as October 2015, more than a year after the initial breach.[49] Assuming, as reports indicate, that the breach occurred sometime before it was detected, hackers had at least a two-year head start to make use of the stolen data.[50] It is important to note, however, that OPM made two rounds of notifications.[51]

Aaron Boyd, *Second OPM Hack Exposed Highly Personal Background Info*, FED. TIMES (June 16, 2015), http://www.federaltimes.com/story/government/omr/opm-cyber-report/2015/06/15/second-opm-hack/71248268/.

[46] *See* Hearing, *supra* note 29 (statement of Katherine Archuleta, Director, Off. Pers. Mgmt.).

[47] *Id.*

[48] Hearing, *supra* note 29 (statement of Robert W. Giannetta, Sr., Chief Information Officer, US Investigations Services, LLC).

[49] *See* COMM. REPORT ON THE OPM DATA BREACH, *supra* note 3, at 5–13 (outlining timeline of key events related to the OPM data breach); and OFF. PERS. MGMT, NEWS RELEASE, *supra* note 21. The author received such notice from the OPM on an undated letter arriving in late October 2015, approximately 20 months after the first sign of trouble at USIS. Letter from the Office of Pers. Mgmt to author (Oct. 2015) (on file with author).

[50] *See* Lynch, *supra* note 2 (discussing damages of cyber identity theft); Stephen Braun, *Security Contractor Breach Goes Unnoticed for Months*, NEWS TO WATCH (Nov. 4, 2014), http://newstowatch.com/news/security-contractor-breach-goes-unnoticed-for-months.html; Lynch, *supra* note 2 (generally discussing damages of cyber identity theft).

[51] *PSC Takes on OPM, FBI Lags on Info Sharing, Joint Chiefs' Email Crashes and More*, FCW (July 30, 2015), https://fcw.com/articles/2015/07/30/news-in-brief-july-30.aspx; Zach Noble, *OPM Breach Notifications, Round Two*, FCW (Aug. 5, 2015), https://fcw.com/articles/2015/08/05/opm-notification-round-2.aspx; *see* COMM. REPORT ON THE OPM DATA

In addition to the delayed employee notifications, there appear to have been early warnings that were ignored, which may have revealed the breach or vulnerabilities leading to the breach sooner.[52] The OPM's own Office of the Inspector General ("OIG") reported a "material weakness related to the lack of IT security and policy procedures" as early as fiscal year 2007.[53] The OIG continued to report on these weaknesses in fiscal years 2009-2013 in their Federal Information Security Management Act ("FISMA") audit reports.[54] While it appears that some strides were made in 2012 and after, the problems clearly resurfaced in 2014, several of which endured well into 2015.[55]

F. *Risks of Intrusion*

The risks posed by this intrusion and data exfiltration stretch beyond traditional identity theft.[56] First, consider the magnitude of the breach. Shortly after the OPM's press release, some news agencies were reporting that the two breaches might have victimized as many as 14 million federal employees.[57]

BREACH, *supra* note 3, at v n. 1 (executive summary noting evidence that indicates that 3.6 million employees' data was impacted by both breaches).

[52] *See* COMM. REPORT ON THE OPM DATA BREACH, *supra* note 3, at 5–13 (outlining first evidence of breach dating back to 2012); Rep. Jason Chaffetz, *The Breach We Could Have Avoided*, THE HILL (Sept. 30, 2015, 7:15 PM), http://thehill.com/special-reports/data-security-october-1-2015/255563-the-breach-we-could-have-avoided ("By ignoring repeated warnings . . . OPM leaders left the agency's valuable data vulnerable to attack.").

[53] Hearing, *supra* note 29, at 35–36 (statement of Michael R. Esser, Asst. Inspector Gen. for Audits, Off. Pers. Mgmt.); *see* COMM. REPORT ON THE OPM DATA BREACH, *supra* note 3, at 14 (outlining multiple findings indicating that OPM's IG identified cybersecurity risks as early as 2005).

[54] *Id.*; U.S. OFF. PERS. MGMT., OFF. INSPECTOR GEN., 4A-CI-00-08-061, FED. INFO. SECURITY MGMT. ACT AUDIT FY 2008; U.S. OFF. PERS. MGMT., OFF. INSPECTOR GEN., 4A-CI-00-09-031, FED. INFO. SECURITY MGMT. ACT AUDIT FY2009; U.S. OFF. PERS. MGMT., OFF. INSPECTOR GEN., 4A-CI-00-10-019, FED. INFO. SECURITY MGMT. ACT AUDIT FY2010; U.S. OFF. PERS. MGMT., OFF. INSPECTOR GEN., 4A-CI-00-11-009, FED. INFO. SECURITY MGMT. ACT AUDIT FY2011; U.S. OFF. PERS. MGMT., OFF. INSPECTOR GEN., 4A-CI-00-12-016, FED. INFO. SECURITY MGMT. ACT AUDIT FY2012; U.S. OFF. PERS. MGMT., OFF. INSPECTOR GEN., 4A-CI-00-13-021, FED. INFO. SECURITY MGMT. ACT AUDIT FY2013.

[55] *See* Hearing, *supra* note 29, at 37 (statement of Michael Esser, Asst. Inspector Gen. for Audits, Off. Pers. Mgmt.); U.S. OFF. PERS. MGMT., OFF. INSPECTOR GEN., 4A-CI-00-15-011, FED. INFO. SECURITY MGMT. ACT AUDIT FY2015; Sara Heath, *OIG Identifies IT Security Issues Following OPM Data Breach*, HEALTH IT SECURITY (Nov. 25, 2015), http://healthitsecurity.com/news/oig-identifies-it-security-issues-following-opm-data-breach.

[56] *See, e.g.*, Lynch, *supra* note 2 (discussing damages of cyber identity theft); Rodin, *supra* note 13, at 507–13 (generally discussing current cyberthreat to critical infrastructure and regulatory efforts to enhance cybersecurity).

[57] *See generally* Erin Kelly, *OPM Still Trying to Determine How Many Hurt by Hack*, USA TODAY (June 16, 2015, 1:28 PM), http://www.usatoday.com/story/ news/politics/2015/06/16/opm-hack-house-hearing-archuleta/71261820/.

One week later, the FBI director, James Comey, estimated that 18 million employees were affected.[58] A September 2015 OPM press release indicated an even higher number: 21.5 million, a number later reported to be 22.1 million by the majority staff of the House Committee on Oversight and Government Reform.[59] The OPM established a cybersecurity incident website that attempted to clarify that the initial breach impacted 4.2 million employees (and that breach notifications to the employees were complete), while the second breach impacted 21.5 million employees (for which notifications started in September 2015 and were expected to go on for 12 weeks).[60] There are numerous implications for such victims, including the exploitation of comprised and sensitive personal data.[61]

Some argue that the population is dangerously ignorant about the risks of cybersecurity incidents.[62] These risks are uniquely and acutely increased when dealing with the cybersecurity workforce (and the federal workforce) given their knowledge, access to information, and sensitivity of many of their positions. The damage wrought could be catastrophic and includes the ability to blackmail,[63] shame,[64] or otherwise coerce public officials.[65]

---

[58] Perez & Prokupecz, *supra* note 40.

[59] *News Release: Statement by OPM Press Secretary Sam Schumach on Background Investigations Incident*, OFF. PERS. MGMT. (Sept. 23, 2015), https://www.opm.gov/news/ releases/2015/09/cyber-statement-923/; COMM. REPORT ON THE OPM DATA BREACH, *supra* note 3, at 14 (outlining multiple findings indicating that OPM's IG identified cybersecurity risks as early as 2005).

[60] *Cybersecurity Incidents*, OFF. PERS. MGMT., CYBERSECURITY RESOURCE CTR., https:// www.opm.gov/cybersecurity/cybersecurity-incidents/#WhatHappened (last visited Nov. 5, 2015).

[61] *See* Elizabeth T. Isaacs, *Exposure Without Redress: A Proposed Remedial Tool for the Victims Who Were Set Aside*, 67 OKLA. L. REV. 519 (2015) (discussing general problems facing victims of data breach to get sufficient redress); Rachael M. Peters, *So You've Been Notified, Now What? The Problem with Current Data-Breach Notification Laws*, 56 ARIZ. L. REV. 1171 (2014) (discussing issues facing victims of data breach).

[62] Michael Kassner, *Ignorance is Not Bliss with Cybersecurity*, TECHREPUBLIC (June 23, 2014, 8:17 AM), http://www.techrepublic.com/article/ignorance-is-not-bliss-with-cybersecurity (quoting P.W. Singer, Senior Fellow at the Brookings Institution and cybersecurity expert); Trevor Trimm, *The Senate, Ignorant on Cybersecurity, Just Passed a Bill About it Anyway*, GUARDIAN (Oct. 27, 2015, 5:48 PM), http://www.theguardian.com/ commentisfree/ 2015/oct/27/senate-ignorant-of-cyber-security-just-passed-cisa-bill-anyway.

[63] *See* James Lindgren, *Unraveling the Paradox of Blackmail*, 84 COLUM. L. REV. 670 (1984) (examining issues related to black mail of and by public officials); Henry E. Smith, *The Harm in Blackmail*, 92 NW. U. L. REV. 861 (1998) (discussing the harm in any type of blackmail).

[64] *See* Toni M. Massaro, *Shame, Culture, and American Criminal Law*, 89 MICH. L. REV. 1880 (1991) (discussing cultural and emotional implications of shaming in a criminal justice context).

One such example is the case of a San Antonio Police Department Captain[66] in the aftermath of the Ashley Madison hack.[67] Captain Michael Gorhum committed suicide after his official email address was included on a published list of purported Ashley Madison users, a website for helping users arrange extramarital affairs.[68] According to reports, Captain Gorhum was not actually on the list of users involved in this breach.[69] However, "when Capt. Gorhum's name was published, he was devastated and his colleagues quickly became aware of his presence on it."[70] This incident illustrates one of the numerous potential harms of the compromise of data related to a public official. In fact, lawmakers recently indicated that they lack a good understanding of the national security risks of such data breaches; therefore, under the House version of the 2016 Intelligence Authorization Act, "the president must deliver a report covering the effects of the cyberintrusion 'on each element of the intelligence community.'"[71]

III. CYBERSECURITY LAW: TRAINING AND REPORTING

This section will survey current law related to cybersecurity training and reporting. Current laws that impact cybersecurity touch on criminal enterprise,[72] privacy,[73] national security,[74] governmental efficiency,[75] executive

---

[65] *See* A. David Pardo et al., *Public Corruption*, 44 AM. CRIM. L. REV. 855 (2007) (exploring public corruption and corruption or impropriety of public officials).

[66] Shekhar Bhatia, *Exclusive: 'Ashley Madison' Suicide Cop Killed Himself After Police-Hating Website Claimed His Email Address was Among Members Even Though it Wasn't Actually on Leaked List*, DAILY MAIL (Aug. 27, 2015, 4:57 PM), http://www.dailymail.co.uk/news/article-3213302/Ashley-Madison-suicide-cop-NOT-leaked-list-cop-hating-website-published-email-address-member-took-life.html.

[67] Robert Hackett, *What to Know About the Ashley Madison Hack*, FORTUNE (Aug. 26, 2015, 7:24 AM), http://fortune.com/2015/08/26/ashley-madison-hack; *Online Cheating Site Ashley Madison Hacked*, KREBS ON SECURITY (July 15, 2015, 8:58 AM), http://krebsonsecurity.com/2015/07/online-cheating-site-ashleymadison-hacked.

[68] *See* Bhatia, *supra* note 66.

[69] *Id.*

[70] *Id.; see also* Sarah D. Katz, *"Reputations . . . A Lifetime to Build, Seconds to Destroy": Maximizing the Mutually Protective Value of Morals Clauses in Talent Agreements*, 20 CARDOZO J. INT'L & COMP. L. 185 (2011) (generally explaining the reputational harm to a public personality of public knowledge that he or she participates in activities such as Ashley Madison advances).

[71] Sternstein, *supra* note 6 (citing Intelligence Authorization Act for Fiscal Year 2016, H.R. 4127, 114th Cong. (2015)).

[72] *See* Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, 98 Stat. 2190 (prohibiting certain types of attacks on government and banking systems); *see, e.g.*, Kayla Morency, *Cybersecurity Finally Takes Center Stage in the U.S.*, 15 J. HIGH TECH. L. 192 (2014) (generally discussing development of cybercrime law).

[73] *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (prohibiting unauthorized electronic surveillance or eavesdropping).

agency policy,[76] research,[77] and information management.[78] A recent Congressional Research Service article by Eric Fisher reviewed legislative efforts to keep pace with cybersecurity, noting that such efforts fit broadly into ten categories.[79] One such category is of particular interest to this topic, which Fisher's article refers to as "the cybersecurity workforce."[80] This is not to discount or ignore classified or other policy that is unavailable to the public, some of which are briefly surveyed by Fisher,[81] but such efforts are beyond the scope of this paper. Additionally, this is not to suggest that the legislative branch remains ignorant of the importance of cybersecurity, as there are several bills or resolutions currently moving through Congress on the matter.[82] We now turn to briefly review a few such efforts.

---

[74] *See* Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (giving the Dept. of Homeland Security some cybersecurity responsibility).

[75] *See* Paperwork Reduction Act of 1980, Pub. L. No. 96-511, 94 Stat. 2812 (requiring the Office of Management and Budget ("OMB") to develop cybersecurity policies).

[76] *See* Clinger-Cohen Act of 1996, Pub. L. No. 104-106, 110 Stat. 642 (giving cybersecurity policy responsibility to agency heads).

[77] *See* Cyber Security Research and Development Act of 2002, Pub. L. No. 107-305, 116 Stat. 2367 (giving cybersecurity responsibilities with research and development to the National Science Foundation and National Institute of Standards and Technology).

[78] *See, e.g.*, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899 (initiating and guiding federal information technology management); Federal Information Security Management Act of 2002, Pub. L. No. 107-347, 116 Stat. 2946 (clarifying agency roles with information security management, shifting primary responsibility from the Department of Commerce to OMB); Computer Security Act of 1987, Pub. L. No. 100-235, 101 Stat. 1724 (dealing with developing security systems for federal computer systems).

[79] ERIC A. FISHER, CONG. RESEARCH SERV., R42114, FEDERAL LAWS RELATING TO CYBERSECURITY: OVERVIEW OF MAJOR ISSUES, CURRENT LAWS, AND PROPOSED LEGISLATION 6 (2014).

[80] *Id.* at 6, 24–25, 53.

[81] *See id.* at 3.

[82] *See, e.g.*, Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. (2015) (as amended by S. 2716, 114th Cong. (2015)) (proposing to enhance information sharing about cybersecurity threats); Department of Homeland Security Cybersecurity Strategy Act of 2015, H.R. 3510, 114th Cong. (2015) (proposing to require the Secretary of the Department to develop a cybersecurity strategy); Promoting Good Cyber Hygiene Act of 2015, H.R. 3664, 114th Cong. (2015) (proposing to require the National Institute of Standards and Technology to identify and document best practices for processes, procedures and mechanisms that help protect information systems); Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act of 2015, H.R. 3878, 114th Cong. (2015) (proposing to increase information sharing related to cybersecurity threats on ports); Strengthening State and Local Cyber Crime Fighting Act, H.R. 3490, 114th Cong. (2015) (proposing to establish a National Computer Forensics Institute).

A. *Clinger-Cohen Act of 1996*[83]

The Clinger-Cohen Act of 1996 ("Clinger-Cohen") was an early effort at what is now considered cybersecurity law and policy.[84] Clinger-Cohen included a division E, entitled "Information Technology Management Reform."[85] While a great deal of Clinger-Cohen dealt with acquisition policies related to information technology, section 5112(i) mentions training: "The Director [of OMB] shall monitor the development and implementation of training in information resources management for executive agency personnel."[86] Section 5113 also required management principles, obliging agency heads to "ensure that the information security policies, procedures, and practices are adequate."[87] Finally, Clinger-Cohen added the designation of a Chief Information Officer to Executive Agencies.[88] Clinger-Cohen did not provide, nor apparently contemplate, reporting requirements for cybersecurity incidents or data breaches.[89]

B. *Homeland Security Act of 2002*[90]

The Homeland Security Act of 2002 ("HSA")—passed in the wake of the terrorist attacks of September 11, 2001—was the largest federal government reorganization since the National Security Act of 1947, creating a new federal department and cabinet-level position.[91] The HSA contained several provisions related to cybersecurity, including a provision to "enhance[ ] non-federal cybersecurity,"[92] the Cyber Security Enhancement Act of 2002,[93] a provision to require the "dissemination of advanced investigative analysis and forensic tools to assist state and local law enforcement agencies in combating cybercrime,"[94]

---

[83] Clinger-Cohen Act of 1996, Pub. L. No. 104-106, 110 Stat. 642 (1996).

[84] *See id.*

[85] *Id.* §§ 5001–703.

[86] *Id.* § 5112(i).

[87] *Id.* § 5113(b)(2)(D).

[88] *Id.* § 5125.

[89] *See id.*

[90] Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002).

[91] *Id.*; National Security Act of 1947, Pub. L. No. 80-253, 61 Stat. 495 (1947); *see also* Jonathan Thessin, *Recent Development: Department of Homeland Security*, 40 HARV. J. LEGIS. 513 (2003) (reviewing the creation of the department); Spencer S. Hsu & Sara Kehaulani Goo, *Homeland Security to be Restructured*, WASH. POST (July 13, 2005), http://www.washingtonpost.com/wp-dyn/content/article/2005/07/12/AR2005071201563.html; Paul C. Light, Opinion, *A Hollow Tribute; The Creation of the Homeland Security Department, Government's Largest Reorganization Since the Truman Days, Likely will be the Most Difficult to Manage*, BROOKINGS (Aug. 2, 2002), https://www.brookings.edu/opinions/a-hollow-tribute-the-creation-of-the-homeland-security-department-governments-largest-reorganization-since-the-truman-days-likely-will-be-the-most-difficult-to-manage/.

[92] Homeland Security Act of 2002, Pub. L. No. 107-296, § 223, 116 Stat. 2135 (2002).

[93] *Id.* § 225 (dealing almost exclusively with criminal matters).

[94] *Id.* § 232(b)(11).

and a provision related to private-sector cybersecurity.[95] Notably absent from the HSA are cybersecurity awareness training or cybersecurity incident and data breach reporting requirements.[96]

C. *Cybersecurity Information Sharing Act of 2015 and Federal Cybersecurity Workplace Assessment Act of 2015*[97]

On December 18, 2015, the President signed into law the Public Law 114-113, the Consolidated Appropriations Act, 2016, which included the Cybersecurity Information Sharing Act of 2015 ("CISA") and the Federal Cybersecurity Workplace Assessment Act of 2015 ("CWAA") that very briefly addressed training the cybersecurity workforce and reporting data breaches.[98] Although this law proposes much more than enhanced information sharing, it only briefly addresses cybersecurity workforce training and education, requiring agencies to develop and assess "a strategy for mitigating any gaps identified in clause (i) or (ii) with the appropriate training and certification for existing personnel."[99] Further, section 109 of the bill also proposes some general, retroactive reporting requirements by mandating certain periodic reports by the Director of National Intelligence in conjunction with other agencies.[100]

IV. GAP ANALYSIS

It appears that most federal agencies are generally left to themselves about whether to even implement policy related to training the workforce on cybersecurity. The law has developed in a direction that appears more focused on acquisition policy[101] and information management and security policy.[102]

---

[95] *Id.* § 892.

[96] *See, e.g.*, John Grant, *Will There be Cybersecurity Legislation*, 4 J. NAT'L SECURITY L. & POL'Y 103, 106 (2010) (generally discussing DHS responsibilities related to cybersecurity under HSA).

[97] Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. (2015) (as amended by S. 2716, 114th Cong. (2015)); *see, e.g.*, Jay P. Kesan & Carol M. Hayes, *Creating a "Circle Of Trust" to Further Digital Privacy and Cybersecurity Goals*, 2014 MICH. ST. L. REV. 1475 (2014) (generally discussing public-private partnerships for cybersecurity).

[98] *See* Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, 129 Stat. 2936 (2015) §§ 301–05 (federal cybersecurity workforce assessment), § 109 (report on cybersecurity threats).

[99] *Id.* § 303(b)(1)(D)(iii).

[100] *Id.* § 109.

[101] *See* Clinger-Cohen Act of 1996, Pub. L. No. 104-106, 110 Stat. 642 (1996).

[102] *See, e.g.*, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899 (2002) (initiating and guiding federal information technology management); Federal Information Security Management Act of 2002, Pub. L. No. 107-347, 116 Stat. 2946 (2002) (clarifying agency roles with information security management, shifting primary responsibility from the Department of Commerce to OMB); Computer Security Act of 1987, Pub. L. No. 100-235,

While CISA starts to address training[103] and privacy concerns,[104] it does not go nearly far enough. Many agencies implement some level of cyber awareness training materials to employees accessing or maintaining their accounts,[105] but those materials often lag behind the threats and fail to capitalize on the collective experience and knowledge of the entire federal government.[106]

Further, there does not appear to be any federal law that relates to reporting data breaches within the federal government. The discussion of the OPM data breach makes clear that timely reporting could have allowed the relevant agencies and affected employees to take steps to protect their interests much sooner than nearly two years later.[107] Some agencies do have publicly available policies related to data breach response, such as the Department of Justice's Instruction 0900.00.01, Incident Response Procedures for Data Breaches ("Incident Response Procedures").[108] The Incident Response Procedures actually require reporting, "within one hour of discovery" of "actual or suspected data breaches" and other related incidents.[109] Such policy is exactly the type needed for cybersecurity in this day and age, but it is not sufficient for each agency to have its own unique requirements.

V. RECOMMENDATIONS

As outlined above, the risk of cybersecurity incidents is not just a digital or technological risk.[110] There are financial costs.[111] There are real people in-

---

101 Stat. 1724 (1987) (dealing with developing security systems for federal computer systems).

[103] *See* Cybersecurity Information Sharing Act of 2015 § 303(b)(1)(D)(iii).

[104] *See* Trimm, *supra* note 62.

[105] *See, e.g.*, U.S. DEP'T OF DEFENSE, DIRECTIVE 8570.1, INFORMATION ASSURANCE TRAINING, CERTIFICATION, AND WORKFORCE MANAGEMENT (2003) (Department of Defense implementing guidance for cyber awareness training); U.S. DEP'T OF JUSTICE, ORDER 2640.2F, INFORMATION TECHNOLOGY SECURITY (2008) (Department of Justice implementing policy and guidance for cyber awareness).

[106] *See* OFF. INSPECTOR GEN., U.S. POSTAL SERV., AUDIT REPORT NO. IT-AR-16-01, INFO. SECURITY AWARENESS TRAINING AND PHISHING (2015) (outlining overwhelmingly poor performance by Postal Service employees on cybersecurity testing); Amanda Vicinanzo, *DHS US Cybersecurity Practices Fail to Keep Pace with Cyber Adversaries*, HOMELAND-SECURITYTODAY.US (Nov. 24, 2014), http://www.hstoday.us/channels/dhs/single-article-page/us-cybersecurity-practices-fail-to-keep-pace-with-cyber-adversaries/170a083812f4f52eb11575675d 8739a0.html; Robert Lemos, *Federal Agencies Fail to Secure Systems: Report*, EWEEK.COM (Feb. 9, 2014), http://www.eweek.com/security/federal-agencies-fail-to-secure-systems-report.html.

[107] *See supra* Part I.

[108] U.S. DEP'T OF JUSTICE, INSTRUCTION 0900.00.01, INCIDENT RESPONSE PROCEDURES FOR DATA BREACHES (2013).

[109] *Id.* at 9.

[110] *See supra* Parts I–II.

[111] *See* Lawrence L. Muir, *Combatting Cyber-Attacks Through National Interest Diplo-*

volved with real human costs. The federal government should not sit back and leave each agency to develop its own unique approaches to cybersecurity awareness and incident reporting. The benefit of a mandatory and uniform approach is that it capitalizes on the collective federal government experience in this field.

A. *Cybersecurity Training*

While the Senate took a step in the right direction by at least mentioning cybersecurity workforce training and education, it is simply not enough.[112] Congress should implement legislation, whether as part of CISA or otherwise, that explicitly requires training and education for the entire federal workforce related to awareness of the various cybersecurity risks and threats. The training must be mandatory for all employees in the federal workforce, which means it must be funded. Such legislation should provide some level of information sharing and coordination allowing for all agencies to compare best practices related to training and education.

Additionally, the training should be centralized and continually updated both in form and content. It should change and evolve along with the cybersecurity threat. I propose vesting this responsibility in some centralized custodian agency or department, perhaps the OPM. Centralizing the training requirements will allow each department and agency to strengthen institutional knowledge and data on both emerging threats and the effectiveness of current training methods. Having one agency responsible for consolidating this information and implementing continually updated training allows for maximum efficiency and avoids duplication of efforts among the different agencies. Recognizing that there may be some classified or sensitive requirements unique to certain agencies (such as within the intelligence community), a built-in mechanism should be established equipping such agencies to supplement the centralized training and education program. Agencies should also be able to opt out of the centralized training, but this waiver would require high-level government approval and be reviewed annually to ensure uniform application. Regardless of waiver, agencies should still be required to forward all unclassified lessons learned about both emerging threats and effectiveness of training.

Further, the importance of continually updating both form and content cannot be understated. Simply requiring employees to conduct the same annual training year after year is not the best approach because such training becomes stale, uninteresting, and decreasingly effective. Rather, the training must be continually updated to discuss and incorporate emerging threats and information, and it must be reviewed periodically for effectiveness.

Lastly, with regard to effectiveness, there must be oversight of this program.

---

macy: A Trilateral Treaty with Teeth, 71 WASH. & LEE L. REV. ONLINE 73, 80–83 (2014) (generally discussing costs of cybercrime in the United States).

[112] *See* Cybersecurity Information Sharing Act of 2015 § 303(b)(1)(D)(iii).

One proposal is to mandate either annual or biannual reviews by each department or agency's inspector general (according to size and resources of the individual inspectors general). Such review and feedback should be provided to the centralized training custodian to ensure that the centralized approach is being uniformly implemented and to gauge its effectiveness. Congress can then review the program periodically to ensure that it is effectively increasing the federal workforce's actual cybersecurity awareness.

B. *Reporting Data Breaches*

Data breaches need to be reported immediately. In fact, this is one area where over-reporting is likely worth the risk of possible misinformation in initial reports. It is better to alert the relevant officials and cybersecurity workforce of suspected breaches sooner rather than later. Immediate investigation is certainly needed to attempt to ascertain the scope and nature of the breach.[113] Potentially affected employees also need notification at the earliest possible opportunity to protect themselves against identity theft and other forms of exploitation.[114]

Unlike training, this requirement must be imposed upon all departments and agencies individually.[115] It must be crafted so that it clearly and decisively requires, as the Incident Response Procedures do,[116] immediate notification for even a suspected data breach. Further, the reporting must be two-fold: notification of appropriate agency officials and notification of potentially impacted employees.[117] This provision can and should be part of the ongoing training requirements discussed above.[118] Specifically, upon suspicion of a data breach, the affected agency can take the opportunity to both notify employees of a suspected breach and refer them to the annual training information and any additional protections implemented in response to the specific threat. It is better to have an initial and incomplete notification to employees, informing them of a possible breach and advising that more information will follow, than to wait until it is decisively determined that there was a breach.[119] Premature notification of a potential breach causes almost no harm beyond inconveniencing employees with a reminder of the cybersecurity age's data risks. Conversely, late notification could subject employees to potential catastrophic exploitation.[120]

---

[113] *See supra* Part I.e.

[114] *See supra* text accompanying notes 50–52.

[115] *See supra* Part IV.a.

[116] *See* U.S. DEP'T OF JUSTICE, *supra* note 108.

[117] *See supra* Part III.

[118] *See supra* Part IV.a.

[119] *See supra* Part I.e.

[120] *See supra* Part I.f.

VI. CONCLUSION

The OPM data breach reminds us that the government's stored information is always at risk and under attack by malign actors. Knowledge of such persistent threats must not be ignored. Likewise, knowledge of relevant threats must be spread through government to the entire cybersecurity workforce through effective and efficient training. Further, mandatory and timely reporting of cybersecurity incidents and data breaches is required so that employees have the best opportunity to protect themselves and the government.[121] In the event that such timely notification does not occur, there needs to be a standard to which officials can be held accountable. These methods may be easier and more cost-effective ways to mitigate cybersecurity risk across the government (compared to various attempts by OPM)[122] and protect the nation's security. Such prophylactic methods can be thought of as rectifying "sloppy cyber hygiene," identified in the wake of the OPM Data Breach.[123]

---

[121] *See supra* Parts I.e. and I.f.

[122] *See* U.S. OFF. PERS. MGMT., OFF. INSPECTOR GEN., 4A-CI-00-16-039, FED. INFO. SECURITY MGMT. ACT AUDIT FY2016 at 7–8 (outlining expenditure of millions of dollars in modernization efforts without results related to background investigations, among other areas); COMM. REPORT ON THE OPM DATA BREACH, *supra* note 3, at v–vi (executive summary discussing non-monetary significance of information stolen in OPM Data Breach).

[123] COMM. REPORT ON THE OPM DATA BREACH, *supra* note 3, at viii (executive summary discussing impact of OPM Data Breach).