National Security Law Journal

Excerpt from Vol. 4, Issue 2 (Spring/Summer 2016)

Cite as:

Chelsea C. Smith, Comment, *Hacking Federal CyberSecurity Legislation: Reforming Legislation to Promote the Effective security of Federal Information Systems*, 4 NAT'L SEC. L.J. 345 (2016).

ISSN: 2373-8464

The *National Security Law Journal* is a student-edited legal periodical published twice annually at George Mason University School of Law in Arlington, Virginia. We print timely, insightful scholarship on pressing matters that further the dynamic field of national security law, including topics relating to foreign affairs, intelligence, homeland security, and national defense.

We welcome submissions from all points of view written by practitioners in the legal community and those in academia. We publish articles, essays, and book reviews that represent diverse ideas and make significant, original contributions to the evolving field of national security law.

Visit our website at www.nslj.org to read our issues online, purchase the print edition, submit an article, or sign up for our e-mail newsletter.

COMMENT

HACKING FEDERAL CYBERSECURITY LEGISLATION: REFORMING LEGISLATION TO PROMOTE THE EFFECTIVE SECURITY OF FEDERAL INFORMATION SYSTEMS

Chelsea C. Smith*

In 2015, the U.S. Office of Personnel Management announced that it had experienced multiple cybersecurity incidents that resulted in the compromise of sensitive information for over 22 million individuals. These breaches represent the worst cyber intrusions in the history of the U.S. Federal Government. Cybersecurity is a growing national security concern, but the United States does not have a sufficient legislative framework to ensure the protection of federal information systems. While the Federal Information Security Modernization Act of 2014, which reformed the Federal Information Security Management Act of 2002, is intended to provide a framework for information security controls for federal agencies, it has been limited and ineffective. Congress must reform legislation to establish meaningful standards, to ensure methods of accountability to promote compliance, and to dedicate appropriate resources to safeguarding federal information systems. Without action, federal systems will remain at risk and become increasingly susceptible to cyber attacks similar—or worse—to the malicious attacks OPM recently faced.

* George Mason University School of Law, J.D. Candidate, May 2018.

"The United States is fighting a cyber war today, and we are losing."[1]

INTRODUCTION

Social Security numbers, dates and places of birth, health information, employment records, financial information, residency details, educational history, personal contacts, and even fingerprints; these are merely samples of the information that an adversary now

[1] Mike McConnell, *Mike McConnell on How to Win the Cyber-War We're Losing*, WASH. POST, Feb. 28. 2010, at B1 (Mike McConnell served as the Director of the National Security Agency from 1992 to 1996 and the Director of National Intelligence from 2007 to 2009).

holds due to a cyber attack on vulnerable U.S. government systems and networks.[2]

In June 2015, the U.S. Office of Personnel Management ("OPM") announced cybersecurity incidents on its systems that resulted in the compromise of sensitive, personally identifiable information ("PII") (e.g., Social Security number, date of birth) for over 22 million individuals.[3] These incidents also included the loss of "less sensitive," public information (e.g., names, phone numbers, and addresses) of countless others.[4] The stolen data represents "a treasure trove of information about everybody who has worked for, tried to work for, or works for the U.S. government."[5]

These breaches have collectively been described as the worst cyber intrusion in the history of the U.S. Federal Government.[6] As

---

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

[3] *See News Release: OPM Announces Steps*, *supra* note 2; *News Release: OPM to Notify Employees*, *supra* note 2.

[4] *See News Release: OPM Announces Steps*, *supra* note 2; *News Release: OPM to Notify Employees*, *supra* note 2. *See also* Sen. Ben Sasse, *Senator Sasse: The OPM Hack May Have Given China a Spy Recruiting Database*, WIRED (July 9, 2015, 5:36 PM), http://www. wired.com/2015/07/senator-sasse-washington-still-isnt-taking-opm-breach-seriously (addressing the types of contacts that individuals provide to OPM when applying for a background investigation).

[5] Ellen Nakashima, *Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say*, WASH. POST (July 9, 2015), https://www.washingtonpost. com/blogs/ federal-eye/wp/2015/07/09/ hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say.

[6] *See, e.g.*, Jason Chaffetz, *The Breach We Could Have Avoided*, THE HILL (Sept. 30, 2015, 7:56 PM), http://thehill.com/special-reports/data-security-october-1-2015/ 255563-the-breach-we-could-have-avoided. *See also* Evan Perez & Shimon Prokupecz, *U.S. Data Hack May be 4 Times Larger than Government Originally Said*, CNN (June 23, 2015, 10:59 PM), http://www. cnn.com/2015/06/22/politics/opm-hack-18-milliion; Tom Risen, *Obama Considers Sanctions After Cyberattacks*, U.S. NEWS & WORLD REPORTS (June 15, 2015, 5:43 PM),

these incidents illustrate, cybersecurity is an area of increasing concern within the national security realm. According to the Director of National Intelligence ("DNI"), "[c]yber threats to U.S. national and economic security are increasing in frequency, scale, sophistication, and severity of impact."[7] As such, there have been significant efforts and investments in building our ability to detect and respond to cyber threats from both domestic and foreign parties.

Despite these efforts, the United States currently lacks an effective cybersecurity legislative framework for the regulation of federal information systems,[8] and the federal functions associated with information security are disjointed and spread across government.[9] While some limited regulatory legislation exists, the government lacks an enforcement mechanism to ensure federal agency compliance with statutory cybersecurity requirements. As a result, government entities are increasingly susceptible to cyber attack, as evidenced by the recent OPM cyber breaches. Congress needs to take legislative action related to cybersecurity to establish a regulatory framework that includes measurable standards for federal agencies to implement. This must include enforcement mechanisms for compliance with established standards, processes to ensure agency accountability for protecting the government's information infrastructure, and added flexibility to government agencies to support recruiting individuals with the expertise to maintain effective information security programs.

This Comment explores cybersecurity legislation that targets the regulation of federal agencies, centering on the Federal Information Security Modernization Act of 2014 ("FISMA 2014"),

---

http://www. usnews.com/news/ articles/2015/06/15/obama-considers-sanctions-after-opm-breach.

[7] James R. Clapper, *Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community*, S. Armed Services Comm. 1 (Feb. 26, 2015).

[8] *See* JOHN ROLLINS & ANNA C. HENNING, CONG. RESEARCH SERV., R40427, COMPREHENSIVE NATIONAL CYBERSECURITY INITIATIVE: LEGAL AUTHORITIES AND POLICY CONSIDERATIONS 4 (2009) ("Legislators and analysts have expressed concerns that the current statutory framework inadequately addresses modern cybersecurity threats.").

[9] *See* ERIC A. FISCHER, CONG. RESEARCH SERV., R43831, CYBERSECURITY ISSUES AND CHALLENGES: IN BRIEF 3 (2014).

which reformed the Federal Information Security Management Act of 2002 ("FISMA 2002") as the primary legislation enacted for regulating federal organizations. This Comment utilizes the recent cyber attacks on OPM as an illustrative example to evaluate this legislation's effectiveness in protecting federal systems and preventing future cyber intrusions from occurring.

Part I provides background on cybersecurity, as well as current and proposed legislation related to the protection of federal systems. Part II describes cybersecurity and the threats that the United States faces in cyberspace. This analysis includes a descriptive overview of cybersecurity, types of cyber threats, where the threats originate, and ways the United States can and has responded to these threats. Part III first discusses the current legislative framework that targets protection of federal systems against cyber attacks, analyzing the effectiveness of FISMA 2002 and its subsequent reform under FISMA 2014. This section next briefly explores the Federal Information Security Management Reform Act of 2015 ("FISMRA 2015"), which a bipartisan group of legislators proposed for enactment following the identification of the OPM cyber incidents. Lastly, to provide a comparison between legislative and executive branch responses, this section addresses Executive Orders to demonstrate how the executive branch has been involved in cybersecurity regulation. Finally, Part IV provides a recommendation for modifying current and proposed legislation to improve the protection of the federal information infrastructure to address the challenges this piece identifies.

I. BACKGROUND: CYBERSECURITY AND THE LAW

This section provides an overview of the term cybersecurity, as it applies to this Comment, particularly in its relation to national security. It concludes with a brief overview of current and pending legislation related to cybersecurity and the protection of federal systems. This section describes the need to take immediate legislative measures to improve our federal information infrastructure.

A. Cybersecurity and its Ties to National Security

Cybersecurity (sometimes referred to as information security) includes the efforts, activities, and processes associated with protecting digital information and critical information systems and infrastructures, including computers, networks, and programs, from unauthorized access.[10] A cyber attack occurs when one or more actors deliberately attempt to access and/or alter computer systems, networks, or information technology programs.[11]

Cybersecurity is becoming one of the largest national security concerns within the United States because cyber attacks present one of the most severe threats to the nation.[12] Recognizing the increased threat of cyber espionage and attack,[13] the White House identified the need to secure the nation's cyberspace as a critical component of its National Security Strategy.[14]

Despite agreement that protection of our nation's information systems is a critical priority, efforts to safeguard federal systems have been lacking.[15] Information stored on federal systems is often sensitive in nature (e.g., tax records containing private financial information, Social Security records, proprietary business information, defense and national security records), and

---

[10] *See* David G. Delaney, *Cybersecurity and the Administrative National Security State: Framing the Issues for Federal Legislation*, 40 J. LEGIS. 251, 251 (2013-2014).
[11] *See, e.g.*, Matthew F. Ferraro, *"Groundbreaking" or Broken? An Analysis of SEC Cybersecurity Disclosure Guidance, Its Effectiveness, and Implications*, 77 ALB. L. REV. 297, 307 (2013-2014) (describing "cyber attack" as the deliberate action to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information in these systems or networks).
[12] *See, e.g.*, 161 CONG. REC. S5456 (daily ed. July 22, 2015) (statement of Sen. Mark Warner); ROLLINS & HENNING, *supra* note 8, at 1 ("Cybersecurity has been called 'one of the most urgent national security problems facing the new administration.'").
[13] *See, e.g.*, Ferraro, *supra* note 11, at 309-10.
[14] THE WHITE HOUSE, NATIONAL SECURITY STRATEGY 1, 3 (2015), https://www.whitehouse.gov/sites/ default/files/docs/2015_national_security_ strategy_2.pdf.
[15] Robert Silvers, *Rethinking FISMA and Federal Information Security Policy*, 81 N.Y.U. L. REV. 1844, 1846 (2006) (identifying that "efforts to secure federal data have been marked by delay, inefficiency, and ineffectiveness").

unauthorized access can be devastating to the government.[16] However, there are limited regulations focused on ensuring cybersecurity of federal systems. And where regulation exists, federal agencies have been slow in satisfying the requirements for information security, and oversight and enforcement of these requirements is weak.[17]

B. Cybersecurity Legislation

The nation's cybersecurity concerns include the ability to protect federal systems and the critical information stored on these systems. In an effort to address these concerns, over the last fifteen years, Congress enacted some regulatory legislation designed to protect federal information systems.

Congress enacted FISMA 2002 following the time-limited Government Information Security Reform Act of 2000 ("GISRA"), in response to the government's ineffective security of federal systems and information.[18] FISMA 2002 had the intended purpose of "provid[ing] a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets."[19] Details in Part III describe how FISMA 2002 focused federal agency efforts on ensuring effective computer security, and protecting against unauthorized access to federal systems.[20] It accomplished this by requiring annual reports to the Office of Management and Budget

---

[16] *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-08-571T, INFORMATION SECURITY: PROGRESS REPORTED BUT WEAKNESSES AT FEDERAL AGENCIES PERSIST 3-4 (2008) [hereinafter GAO-08-571T]; Silvers, *supra* note 15, at 1845.

[17] *See, e.g.*, GAO-08-571T, *supra* note 16, at 3.

[18] *The Federal Information Security Management Act of 2002: Hearing on H.R. 3844 Before the Subcomm. on Gov't Efficiency, Fin. Mgmt and Intergovernmental Relations of the Comm. On Gov't Reform*, 107th Cong., 42 (2002) [hereinafter Hearing on H.R. 3844] (Rep. Thomas Davis stated, "I am not satisfied with our Federal Government's overall performance in securing our information infrastructure. The bottom line is, we are still too vulnerable.").

[19] Purposes, 44 U.S.C. § 3541 (2012). Information security refers to "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction." Definitions, 44 U.S.C. § 3542(b)(1) (2012).

[20] Hearing on H.R. 3844, *supra* note 18, at 40-41.

("OMB"), the development of information security standards by the National Institute of Standards and Technology ("NIST"), and the creation of an information security incident center.[21] FISMA 2002 also mandated federal agencies to establish a Chief Information Officer ("CIO") position tasked with protecting the agency's computer systems from unauthorized access and cyber attacks.[22]

However, agencies encountered several challenges that limited the ability to achieve the goals of FISMA 2002. For example, FISMA 2002 assigned multiple federal agencies responsible for implementing the law, and agencies were unable to keep up with the ever-increasing threat of cyber attack from criminals, terrorists, and foreign state actors.[23] Addressing these challenges, Congress enacted FISMA 2014 to update FISMA 2002. Congress intended for this update to clarify and codify the roles of OMB and the U.S. Department of Homeland Security ("DHS"). It provided OMB the authority to oversee and manage information security across federal agencies, and formally established DHS as the agency responsible for executing the operational aspects of federal cybersecurity through the monitoring of federal systems.[24] FISMA 2014 also adjusted the way the government managed federal data breaches, by increasing transparency and establishing uniformity in the process for reporting cyber incidents.[25]

Despite these legislative changes regulating the information security of federal systems, the federal information infrastructure remains vulnerable to cyber attacks, as evidenced by the recent OPM cybersecurity incidents. Following these breaches, FISMRA 2015 was proposed. FISMRA 2015 seeks to reform FISMA 2014, by allowing DHS to operate intrusion detection capabilities on all federal agencies within the "dot-gov" domain, directing DHS to conduct risk assessments of networks within this federal purview, and requiring

---

[21] *Id.*
[22] Federal Agency Responsibilities, 44 U.S.C. § 3544 (2012); *see also* ROLLINS & HENNING, *supra* note 8, at 9.
[23] S. REP. NO. 113-256, at 2 (2014).
[24] *Id.* at 3-4.
[25] *Id.* at 7-8.

regular reports from OMB to Congress on the execution of their enforcement authorities under the statute.[26]

While FISMRA 2015 addressed some of the weaknesses of existing legislation, neither the proposal nor current law establishes strong cybersecurity standards and enforcement mechanisms under which federal agencies must comply. The current cybersecurity legislative framework is not working, and the nation's federal systems remain vulnerable to attack.[27] Until federal agencies are held accountable to strong standards for information security management, it is likely government agencies will remain susceptible to cyber attack.

II. CYBERSECURITY: THREATS AND RESPONSES

This section provides a detailed analysis of ongoing cybersecurity threats that the United States faces. This analysis includes a descriptive overview of cybersecurity, the types of existing cybercrimes and threats, who the primary threats are, and ways the United States can respond to these threats. This section sets the stage for the following section's discussion of the legislative actions that the United States implemented to protect federal systems from cyber threats.

A. The Threat of Cybercrime

Cyberspace, a necessary element of our economy and national security, serves as "the control system of our country" as it allows the United States' critical infrastructure to operate.[28] Countless

---

[26] 161 CONG. REC. S5456 (daily ed. July 22, 2015) (statement of Sen. Collins).
[27] Gus P. Coldebella & Brian M. White, *Foundational Questions Regarding the Federal Role in Cybersecurity*, 4 J. NAT'L SECURITY L. & POL'Y 233, 236 (2010).
[28] Melanie J. Teplinsky, *Fiddling on the Roof: Recent Developments in Cyber Security*, 2 AM. U. BUS. L. REV. 225, 233 (2012-2013) (quoting the DHS 2003 National Security Strategy to Secure Cyberspace). "Critical infrastructure" in this context refers to the "systems and assets so vital to the United States that their incapacity or destruction would have a debilitating impact on national security." U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-15-714, FEDERAL INFORMATION SECURITY: AGENCIES NEED TO CORRECT WEAKNESSES AND FULLY IMPLEMENT SECURITY PROGRAMS 1 n.1 (2015) [hereinafter GAO-15-714].

interconnected computers, servers, and cables comprise cyberspace.[29] "Cyberspace affects every aspect of daily life."[30] However, the growth of technology, computing, and networking led to advances in crime within this cyberspace.[31] Crime in cyberspace is unique because the use of computers to perpetrate a crime is often less expensive, the internet makes it easier for criminals to communicate, and the activities are frequently undetected.[32] Cybercrime ranges from unauthorized access to computer programs, to disruption—and even destruction—of these files or programs, to actual theft of information and/or identities.[33] Cybercrime also includes cyber terrorism, which consists of any criminal or terrorist attack conducted in cyberspace that results in violence or destruction of its target and has the purpose of inciting terror and/or coercing a government.[34] Thus, securing the components of our nation's cyberspace is essential to our national security.[35]

Simply put, cybersecurity is the defense against cyber attacks and cybercrime.[36] Cyber attacks are occurring with increasing frequency, and, as such, have become a principal concern to national and homeland security communities.[37] The ability to destroy or impair virtual systems and assets that are vital to the U.S. national security could have a "debilitating impact on security, national economic security, national public health and safety, or any

[29] Teplinsky, *supra* note 28.
[30] Kelly A. Gable, *Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent*, 43 VAND. J. TRANSNAT'L L. 57, 73 (2010).
[31] *See, e.g.*, Eric G. Orlinsky, *Cyber Security: A Legal Perspective*, MD. B. J. 33, 34 (2014) ("The threat of a cyber attack and the extent of potential danger to an organization continues to grow with daily technological innovations."); Teplinsky, *supra* note 28.
[32] *See* Gable, *supra* note 30, at 60; Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003, 1006-08 (2001).
[33] *See, e.g.*, Katyal, *supra* note 32, at 1013.
[34] Gable, *supra* note 30, at 62-63.
[35] Teplinsky, *supra* note 28.
[36] *See* Delaney, *supra* note 10; Stephen Dycus, *Congress's Role in Cyber Warfare*, 4 J. NAT'L SECURITY L. & POL'Y 155, 162 (2010); Gable, *supra* note 30, at 62-63.
[37] *See* Gable, *supra* note 30, at 60; ROLLINS & HENNING, *supra* note 8, at 2-3.

combination of those matters."[38] Admiral Michael Mullen, the former Chairman of the Joint Chiefs of Staff, described cyber threats as one of "two existential threats to the United States," with the other being nuclear proliferation.[39] A sophisticated cyber attack, similar to a nuclear attack, would likely come without clear warning and, because of a lack of a reliable and effective defense mechanism, would cause extensive, long lasting, and indiscriminate direct and indirect damage.[40]

Cyber war is becoming a reality,[41] and the United States is not prepared to defend against a sophisticated attack.[42] Actors engage in cyber terrorism or espionage where they use cyberspace to gather intelligence and information critical to national and economic security.[43] The U.S. information infrastructure serves as a constant target for cyber attack.[44] For example, on any given day, the U.S. Department of Defense experiences millions of attempted cyber attacks.[45] Over the last several years, cyber attackers have successfully accessed and compromised sensitive government and military information. For instance, over a two-year period, hackers obtained confidential files regarding the military's fighter aircraft from the U.S. Air Force's air traffic control systems.[46] These cyber attacks will

[38] ROLLINS & HENNING, *supra* note 8, at 2-3; *see also* Gable, *supra* note 30, at 74 ("Without ever having to build a bomb or sacrifice themselves, cyberterrorists can bring down the critical infrastructure of an entire state, disrupt the global economy, and instill fear and chaos among billions of people.").
[39] Ferraro, *supra* note 11, at 309.
[40] Dycus, *supra* note 36, at 163.
[41] Peter M. Shane, *Cybersecurity: Toward a Meaningful Policy Framework*, 90 TEX. L. REV. 87, 89 (2012).
[42] John S. Fredland, *Building a Better Cybersecurity Act: Empowering the Executive Branch Against Cybersecurity Emergencies*, 206 MIL. L. REV. 1, 4 (2010) (Mike McConnell, former Director of National Intelligence, claimed that U.S. adversaries have the ability to bring down a power grid through cyberattack and the "United States is not prepared for such an attack.").
[43] ROLLINS & HENNING, *supra* note 8, at 1.
[44] *See* Fredland, *supra* note 42, at 3; *see also* Mike Mount, *Hackers Stole Data on Pentagon's Newest Fighter Jet*, CNN (Apr. 21, 2009), http://edition.cnn.com/2009/US/04/21/pentagon.hacked (addressing an increase in attacks on U.S. military and government networks).
[45] *See, e.g.*, Fredland, *supra* note 42, at 3 ("On a single day in 2008, the Pentagon experienced six million attacks from would-be cyberintruders.").
[46] Mount, *supra* note 44.

only increase in sophistication.[47] "As cyberspace evolves, it is increasingly likely that threat actors can remotely cause kinetic attacks, disrupt vital national systems, or diminish government response capabilities."[48] Some senior government officials claim that the cyber attacks on the OPM systems and networks, and the resulting theft of data, should be called an act of war that requires retaliatory action.[49]

Protecting our vulnerabilities now plays a critical role in our national security strategy.[50] "Protecting networks, computers, programs, and data—and the critical infrastructures on which they rely—from attack, damage, or unauthorized access could hardly be more important."[51] The White House recently identified a focus of "fortifying our critical infrastructures against all hazards, especially cyber espionage and attack" in the U.S. National Security Strategy.[52] President Obama separately identified cyber attacks as "one of the most serious economic and national security challenges" facing our nation.[53] As cybercrime continues to increase in volume and degree of sophistication, it is likely the federal government will remain focused on strategically deterring against these cyber attacks and protecting its federal systems.

B. Sources of Cyber Threats

As cyberspace continues to grow, the type of crime and actors involved in cybercrime continues to evolve as well.[54] Cyber threats may come from a range of actors including foreign nation

---

[47] Shane, *supra* note 41.
[48] Delaney, *supra* note 10, at 257.
[49] Tom Leithauser, *OPM Cyber Attack was 'Act of War,' U.S. Should Retaliate, McCain Says*, CYBERSECURITY POL'Y REP. (2015).
[50] *See* Teplinsky, *supra* note 28, at 232 ("Our shared digital infrastructure is vulnerable to a wide-range of cyberthreats that are understood to pose some of the most serious economic and national security challenges of the 21st century.").
[51] Shane, *supra* note 41, at 87.
[52] THE WHITE HOUSE, *supra* note 14, at 3.
[53] Barack Obama, *Taking the Cyberattack Threat Seriously*, WALL ST. J. (July 19, 2012, 7:15 PM), http://www.wsj.com/articles/SB10000872396390444330904577535492693 044650.
[54] *See* Clapper, *supra* note 7, at 1.

states with sophisticated programs, nations with lesser technological capabilities but potentially a more hostile intent, criminals motivated for profit, and ideological extremists.[55] Thus, cybercrime may range from phishing attempts on individual citizens for financial gain to "advanced persistent threats," which are highly targeted malware attacks against government and military networks.[56]

Foreign actors have had increased success in recent years in obtaining access to critical infrastructure systems of the United States, but distinguishing actors has become difficult as coordination among foreign nation states expands and the skills and tools used to commit cybercrime develop.[57] According to a 2011 National Counterintelligence Executive Report, Chinese actors are the "the world's most active and persistent perpetrators of [cyber] economic espionage."[58] Similarly, Russia is establishing a cyber command that will conduct offensive cyber activities, such as inserting malware into enemy systems.[59] Other foreign cyber threats include Iran, North Korea, and various terrorist groups.[60] While the federal government and the Obama Administration have not attributed responsibility for the cyber intrusions on the OPM systems, unofficial sources have linked these attacks to China,[61] and this is not the first time officials have suspected China suspected of targeting OPM databases.[62]

---

[55] *Id.*; *see also* GAO-08-571T, *supra* note 16, at 5 (providing a list of sources of cyber threats prepared by the Federal Bureau of Investigation).
[56] *See* Teplinsky, *supra* note 28, at 256-57; *see also* GAO-15-714, *supra* note 28, at 1 ("[A]dvanced persistent threats—where an adversary that possesses sophisticated levels of expertise and significant resources can attack using multiple means such as cyber, physical, or deception to achieve its objectives—pose increasing risks.").
[57] Clapper, *supra* note 7, at 2.
[58] Teplinsky, *supra* note 28, at 260.
[59] Clapper, *supra* note 7, at 2.
[60] *Id.*
[61] *See* Ellen Nakashima, *Chinese Breach Data of Four Million Federal Workers*, WASH. POST (June 4, 2015), https://www.washingtonpost.com/world/national-security/chinese-hackers-breach-federal-governments-personnel-office/2015/06/04/ 889c0e52-0af7-11e5-95fd-d580f1c5d44e_story.html.
[62] Michael S. Schmidt, et al., *Chinese Hackers Pursue Key Data on U.S. Workers*, N.Y. TIMES (July 9, 2014), http://www.nytimes.com/2014/07/10/world/asia/chinese-hackers-pursue-key-data-on-us-workers.html (discussing that, in a previous cyber beach of OPM's systems, the Chinese were accused of targeting employee files for

C. Responding to Cyber Threats and Preventing Cyber Attacks

Identifying the actor involved in a cyber attack can aid in determining the United States response following the attack.[63] For example, if the government determines financial gain or commercial purposes motivated an individual or group of cyber-attackers to seek out data, law enforcement may use traditional criminal justice tools for punishment.[64] However, if the United States is able to identify a foreign nation state as the perpetrator, it is unlikely that the United States will press criminal charges; rather, the response will likely include counterintelligence or military efforts.[65]

The last few Presidential Administrations also attempted to respond to the increase in cyber attacks in various ways.[66] President Clinton established the Critical Infrastructure Protection and the Presidential Information Technology Advisory Council.[67] President George W. Bush created the DHS and tasked the agency with cybersecurity,[68] and he established the Comprehensive National Cybersecurity Initiative to create a defense against network intrusion and strengthen the national cybersecurity environment.[69] President Obama appointed the first Federal CIO to identify and promote efficiencies related to information technology and cybersecurity.[70] Additionally, the Obama Administration released the International Strategy for Cyberspace to promote the flow of information on the internet while ensuring the security of data.[71]

---

those that had applied for Top Secret security clearances).

[63] KRISTIN FINKLEA ET AL., CONG. RESEARCH SERV., IN10287, CYBER INTRUSION ON U.S. OFFICE OF PERSONNEL MANAGEMENT 2 (June 5, 2015).

[64] *Id.* at 2-3.

[65] *Id.*

[66] Delaney, *supra* note 10, at 253.

[67] Gable, *supra* note 30, at 75.

[68] *See* Exec. Order No. 13,228, 66 Fed. Reg. 51,812 (Oct. 8, 2001) (establishing the Office of Homeland Security and charging this office with the protection of information systems); Homeland Security Act of 2002, Pub. L. No. 107-296, §§ 221-25, 116 Stat. 2135, 2155-59 (2002).

[69] Gable, *supra* note 30, at 75-76.

[70] THE WHITE HOUSE: TECHNOLOGY, https://www.whitehouse.gov/issues/technology (last visited Dec. 28, 2015).

[71] *Id.*

In addition to these executive branch responses, an effective legislative framework is a necessary element to ensuring the government can protect U.S. systems and networks from cyber threats.[72] Within the legislative branch, there has been a focus on increasing transparency by sharing information related to cyber attacks, particularly within the private sector, as barriers to information sharing are considered a limitation to effective cybersecurity.[73] For example, the 114th Congress introduced at least three bills that related to the sharing of information among private entities to protect information systems from unauthorized access.[74] Despite these recent efforts, Congress took little action. Currently, an effective framework of legislation for cybersecurity and the protection of federal systems and information infrastructure does not exist.[75]

The government must implement offensive and deterrent strategies to prevent cyber attacks from occurring. "What we need is a long-term, intelligence-driven strategy for safeguarding sensitive, personal information and for deterring future attacks."[76] To do this, Congress needs to reform cybersecurity legislation to develop meaningful standards, provide a means of accountability, and ensure appropriate resources are dedicated to safeguarding federal information systems.

III. CYBERSECURITY LEGISLATION: THE EVOLUTION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT

This section provides an overview of the current legislative framework that targets the protection of federal systems from cyber attacks, as well as the recent proposals to reform this legislation. This includes a discussion of the legislative branch's role in cybersecurity,

---

[72] *See* Dycus, *supra* note 36, at 155.

[73] ERIC A. FISCHER, CONG. RESEARCH SERV., R44069, CYBERSECURITY AND INFORMATION SHARING: COMPARISON OF H.R. 1560 (PCNA AND NCPAA) AND S. 754 (CISA) 1 (2015); Teplinsky, *supra* note 28, at 277 ("More recently, Congress and federal regulators have adopted a number of legislative and regulatory measures to improve transparency with respect to cyber incidents.").

[74] FISCHER, *supra* note 73.

[75] Delaney, *supra* note 10, at 276.

[76] Sasse, *supra* note 4.

an in-depth analysis of FISMA 2002, as well as its reform through FISMA 2014, including its purpose, structure, and criticisms of it. This section then reviews FISMRA 2015 and compares this proposed legislation with existing legislation to identify how it would modify the regulatory framework if the legislature enacted it. For comparison, this section also briefly explores how the executive branch has been involved in responding to cyber threats.

A. Role of the Legislative Branch in Cybersecurity

Congress is responsible for developing legislation to protect against, and respond to, cyber threats, particularly in the face of a potential cyber war. "If Congress is to be faithful to the Framers' vision of its role in the nation's defense, it must tighten its grip and play a significant part in the development of policies for war on a digital battlefield. It also must enact rules to help ensure that these policies are carried out."[77]

Cybersecurity legislation has predominantly focused on the protection of private entities, as the private sector owns and operates the majority of the United States critical information infrastructure.[78] Legislation in this area targeted information sharing between private corporations and the federal government, including the disclosure of security breach information.[79] Specifically, the federal government, and the majority of states enacted data breach notification laws, under which private corporations and public entities must disclose

[77] Dycus, *supra* note 36, at 155.
[78] Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503, 1506 (2013) ("America's critical infrastructure, approximately 85% of which is owned by private firms, already faces constant intrusions.").
[79] *See id.*

data breaches that involve the compromise of sensitive information and PII.[80]

However, limited cybersecurity legislation and regulation addresses federal cybersecurity requirements or focuses on the protection of the federal information infrastructure.

> Part of our cybersecurity problem is institutional—we do not have organizations and practices in place to provide anything like efficient and effective governance in the cybersecurity area. But another huge part is regulatory. We simply do not have in place a framework of laws and regulations, 'smart' or otherwise, that adequately incentivizes the parties with the greatest capacity to improve our security to do so.[81]

Further, cyber attacks on government information infrastructures are increasing in frequency and sophistication, and a successful attack could be devastating.[82] Despite this grave call for action, there has been a great degree of inaction by Congress.[83] FISMA 2002, and subsequent reforms, serve as the only significant framework to ensure the information security of federal systems.[84]

---

[80] Alabama, New Mexico, and South Dakota remain the only states without security breach notification laws. *See Security Breach Notification Laws*, NAT'L CONF. OF STATE LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last updated Oct. 22, 2015) (indicating that as of October 2015, 47 states, the District of Columbia, Puerto Rico, Guam, and the Virgin Islands have enacted data breach notification laws); *see also* Notification in the Case of Breach, 42 U.S.C. § 17932 (2012) (federal data breach notification law).

[81] Shane, *supra* note 41, at 95.

[82] ROLLINS & HENNING, *supra* note 8, at 2 ("Of paramount concern to the national and homeland security communities is the threat of a cyber related attack against the nation's critical government infrastructures . . . so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health and safety, or any combination of those matters.").

[83] *See, e.g.*, FISCHER, *supra* note 9, at 3 ("However, until the end of the 113th Congress, no bills on cybersecurity had been enacted since the Federal Information Security Management Act (FISMA) in 2002.").

[84] Delaney, *supra* note 10, at 277.

B. Federal Information Security Management Act of 2002

1. Overview of FISMA 2002

Congress enacted FISMA 2002 as Title III of the E–Government Act of 2002[85] in response to growing economic and national security concerns, and interests related to information security in the United States.[86] FISMA 2002 codified many aspects of the expiring GISRA,[87] and Congress intended FISMA 2002 to serve as legislative guidance to federal agencies in the development, promulgation, and compliance with management controls for information systems.[88] FISMA 2002 strengthened the requirements established under GISRA through the additional requirement for annual assessments of the effectiveness of information security systems, and the implementation of information security standards.[89] FISMA 2002 established mandatory minimum information security standards for all agencies; it required annual reports to OMB and the Comptroller General, exempting national security and intelligence related systems; and it required the establishment of a federal information security incident center, the United States Computer Emergency Readiness Team.[90] FISMA 2002 was supposed to serve as a comprehensive framework for ensuring effective security controls of federal information systems through various risk management activities.[91]

---

[85] E-Government Act of 2002, Pub. L. No. 107-347 (2003).
[86] *FISMA: Detailed Overview*, NAT'L INST. OF STANDARDS AND TECH., http://csrc.nist.gov/groups/SMA/fisma/ overview.html (last updated Apr. 1, 2014).
[87] PATRICK D. HOWARD, FISMA PRINCIPLES AND BEST PRACTICES: BEYOND COMPLIANCE 7 (2011) ("GISRA required each department or agency head to ensure that information security was provided throughout the life cycle for all agency information systems, and to ensure that agency officials assessed the effectiveness of the information security program, including the testing of information security controls.").
[88] Hearing on H.R. 3844, *supra* note 18, at 43 (statements by Rep. Thorner).
[89] HOWARD, *supra* note 87, at 8.
[90] Hearing on H.R. 3844, *supra* note 18, at 43 (statements by Rep. Thorner).
[91] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-12-137, INFORMATION SECURITY: WEAKNESSES CONTINUE AMID NEW FEDERAL EFFORTS TO IMPLEMENT REQUIREMENTS 2 (2011) [hereinafter GAO-12-137].

FISMA 2002 mandated that federal agencies develop information security strategies to protect their information systems by conducting assessments to identify vulnerabilities to attack, determining the magnitude of the potential harm that would result from cyber attack, and implementing appropriate safeguards to prevent such attacks.[92] Specifically, FISMA 2002 required each agency to "develop, document, and implement an agency wide information security program . . . to provide information security for the information and information systems that support the operations and assets of the agency."[93] FISMA 2002 placed these responsibilities on federal agencies with the presumption that agency officials (namely, CIOs) had the capability to understand risks and other factors related to information security that adversely affected their mission.[94]

2. Distribution of Responsibilities under FISMA 2002

FISMA 2002 assigned specific responsibilities to OMB, NIST, and federal agencies in its attempt to strengthen federal information technology systems. To ensure compliance with the statute, FISMA 2002 identified OMB as having oversight authority over agency actions, the development of information security programs, and the coordination with NIST in the development of information security standards and guidelines.[95] OMB's duties included reviewing agency plans for implementation of the FISMA 2002 requirements, receiving periodic updates from agencies on the status of their compliance, and submitting annual reports to Congress.[96] OMB was also responsible for developing policies and guidelines on information security, and providing instructions to federal agencies for preparing annual reports.[97] Under FISMA 2002, OMB had the power to enforce requirements through a variety of

[92] *See* Delaney, *supra* note 10, at 261; *see also* Silvers, *supra* note 15, at 1848.
[93] Federal Agency Responsibilities: Agency Program, 44 U.S.C. § 3544(b) (2006) (repealed 2014).
[94] *FISMA: Detailed Overview*, *supra* note 86.
[95] Authority and Functions of the Director, 44 U.S.C. § 3543(a) (2006) (repealed 2014).
[96] 44 U.S.C. § 3543(a)(8)(B)-(C) (repealed 2014); *see also* Silvers, *supra* note 15, at 1848-49.
[97] *See* GAO-08-571T, *supra* note 16, at 7.

sanctions and tools, including recommending a decrease in information resources or appropriations for agencies not complying with the requirements.[98] OMB's efforts to date primarily related to issuing guidance to agencies for reporting on a variety of metrics and measuring agency performance against these metrics, which are designed to evaluate agency compliance with FISMA 2002.[99]

FISMA 2002 tasked NIST with developing information security standards and guidelines for use by federal agencies.[100] This includes establishment of information system categories and the minimum requirements for federal information and information systems. As such, NIST established a "risk management framework" to consolidate the security standards and guidelines that FISMA 2002 required for agency use in their development of an information security program and risk management.[101] While this framework does not provide a "one-size-fits-all" approach to cybersecurity, it provides a broad, flexible, cost effective method for agencies to use in managing their cybersecurity risk.[102] However, use of the framework is not mandatory, nor enforced.[103]

Federal agencies are responsible for complying with FISMA 2002 and related policies, procedures, and guidelines and ensuring the overall agency strategic planning process incorporates information security management.[104] More specifically, each agency must maintain an information security program that is commensurate with its risk profile and the magnitude of harm that could result from unauthorized access to that agency's information

[98] Performance-based and Results-based Management: Enforcement of Accountability—Specific Actions, 40 U.S.C. § 11303(b)(5)(B) (2002); *see also* Silvers, *supra* note 15, at 1849.
[99] *See* GAO-15-714, *supra* note 28, at 6; OFFICE OF MGMT & BUDGET, EXEC. OFFICE OF THE PRESIDENT, ANNUAL REPORT TO CONGRESS: FEDERAL INFORMATION SECURITY MANAGEMENT ACT 9 (Feb. 27, 2015) [hereinafter OMB FY14 FISMA Report].
[100] 44 U.S.C. § 3543(a)(3) (2006) (repealed 2014).
[101] *FISMA: Detailed Overview*, *supra* note 86.
[102] Orlinsky, *supra* note 31, at 37.
[103] *Id.*
[104] 44 U.S.C. § 3544 (2006) (repealed 2014); *see also* Howard, *supra* note 87, at 10.

systems.[105] Therefore, each agency must conduct regular assessments of the risk posed to their information security programs, ensure risk-based policies and procedures are in place, establish plans for ensuring adequate information security, provide training for agency personnel on the appropriate use of information systems, and establish a process for identifying and addressing deficiencies to information systems.[106]

Each agency must also establish a CIO and a senior agency information security officer, who most agencies have designated as the Chief Information Security Officer ("CISO"), and agency heads must delegate to these individuals the necessary authority to ensure compliance under FISMA 2002.[107] The CIO and CISO's responsibilities include the development and maintenance of agency information security programs and policies, training of personnel in this functional area, and administration of advice and guidance to senior agency officials related to information security.[108]

In 2010, OMB gave DHS primary responsibility for the operational aspects of federal cybersecurity covered by FISMA 2002,[109] and in 2013, OMB assigned DHS the added responsibility of monitoring federal information systems with the intent of improving the government's ability to more immediately identify emerging cyber threats.[110] DHS must work with each agency to establish an information security continuous monitoring program.[111] OMB requires that these programs be designed to maintain DHS and

---

[105] 44 U.S.C. § 3544. *See also* GAO-08-571T, *supra* note 16, at 6; OMB FY14 FISMA Report, *supra* note 99, at 9.
[106] *See* GAO-08-571T, *supra* note 16, at 6-7.
[107] 44 U.S.C. § 3544(a)(3) (2006) (repealed 2014); *see also* HOWARD, *supra* note 87, at 10.
[108] HOWARD, *supra* note 87, at 11.
[109] OFFICE OF MGMT & BUDGET, EXEC. OFFICE OF THE PRESIDENT, OMB M-10-28, CLARIFYING CYBERSECURITY RESPONSIBILITIES AND ACTIVITIES OF THE EXECUTIVE OFFICE OF THE PRESIDENT AND THE DEPARTMENT OF HOMELAND SECURITY 1 (2010) [hereinafter OMB M-10-28].
[110] OFFICE OF MGMT & BUDGET, EXEC. OFFICE OF THE PRESIDENT, OMB M-14-03, ENHANCING THE SECURITY OF FEDERAL INFORMATION AND INFORMATION SYSTEMS 2 (2013) [hereinafter OMB M-14-03].
[111] *Id.* at 4.

agency awareness of information security, vulnerabilities, and risks, providing the government with the ability to respond in real-time to emerging cyber threats.[112] Following this shift in responsibilities to DHS, DHS began issuing guidance on the information security requirements and metrics for agencies to report on annually.[113]

3. Required Assessments and Reports Under FISMA 2002

FISMA 2002 required government agencies to provide an annual report to OMB, several congressional committees, and the Comptroller General.[114] This report described the effectiveness and adequacy of agency information security programs and policies, including compliance with the requirements established under FISMA 2002.[115] OMB, in turn, provided an annual report to Congress summarizing the independent assessments of agency information security programs (described below), evaluating agency compliance with the standards established by NIST, and identifying significant agency deficiencies in information security practices.[116] In addition to the annual reports, FISMA 2002 requires agencies to include information on security programs and standards in annual budget reports, program performance reports, financial management systems, and information technology management systems.[117]

In September 2009, OMB established a task force to review agency compliance with FISMA 2002, and develop metrics for agency reporting related to information security performance in an effort to advance the security posture of federal agencies.[118] As a result of this task force, OMB implemented a three-tiered approach to reporting under FISMA 2002, which included: data feeds directly from approved security management tools, government-wide

[112] *Id.* at 2.
[113] GAO-15-714, *supra* note 28, at 8.
[114] 44 U.S.C. § 3544(c) (2006); *see also* HOWARD, *supra* note 87, at 29.
[115] 44 U.S.C. § 3544(c); *see also* HOWARD, *supra* note 87, at 15.
[116] HOWARD, *supra* note 87, at 29.
[117] *Id.* at 16.
[118] OFFICE OF MGMT & BUDGET, EXEC. OFFICE OF THE PRESIDENT, OMB M-10-15, FY 2010 REPORTING INSTRUCTIONS FOR THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT AND AGENCY PRIVACY MANAGEMENT 1 (2010) [hereinafter OMB M-10-15].

benchmarking based on agency responses to questions related to its security posture, and agency-specific interviews conducted by a team of government security specialists to identify specific threats based on unique missions.[119] The three-tiered approach in agency reporting aimed at "implementing solutions that actually improve security," rather than a "culture of paperwork reports."[120] OMB maintained responsibility for submitting the annual FISMA report to Congress and made DHS responsible for overseeing agency compliance with FISMA 2002 and agency implementation of, and reporting on, cybersecurity policies and guidance.[121]

FISMA 2002 also mandated that each agency, through its Inspector General ("IG") or independent external auditors, conduct an annual independent evaluation of agency information security programs to determine the effectiveness of these programs.[122] Specifically, the IGs evaluate agency compliance with the statute, measure the effectiveness of information security programs through assessments of information security policies and practices, and identify vulnerabilities to agency information security programs.[123] Under FISMA 2002, agencies submit these evaluations annually to OMB.[124]

C. Federal Information Security Modernization Act of 2014

In December 2014, Congress decided to reform FISMA 2002 through the enactment of FISMA 2014 with the goal of improving federal cybersecurity.[125] FISMA 2014 maintained the same purpose as FISMA 2002, which was to provide a "comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets"

---

[119] *Id.* at 2-3.
[120] *Id.* at 3.
[121] OMB M-10-28, *supra* note 109, at 1-2.
[122] GAO-08-571T, *supra* note 16, at 8.
[123] 44 U.S.C. § 3545 (2006) (repealed 2014); HOWARD, *supra* note 87, at 16-17.
[124] GAO-08-571T, *supra* note 16, at 8.
[125] The Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283 (2014) (amending chapter 25 of Title 44, United States Code, and superseding the very similar Federal Information Security Management Act of 2002).

through government-wide management and oversight of information security risks and programs.[126] Congress intended FISMA 2014 to enhance and modernize the legislative framework for federal information security by clarifying and delegating responsibilities to OMB, DHS, NIST, agency heads, agency CIOs, agency CISOs, and agency IGs.[127]

FISMA 2014 updated FISMA 2002 specifically by clarifying OMB's oversight authority, including the authority to develop and oversee the implementation of information security policies; codifying DHS' authority to administer information security policies and provide technical assistance to federal agencies in the implementation of FISMA requirements; and simplifying reporting requirements to eliminate inefficient and wasteful reporting.[128] FISMA 2014 also reinforced FISMA 2002's requirement that agency heads provide information security programs and protections commensurate with their agency's risk profile.[129]

FISMA 2014 included a new section defining federal agency responsibilities, reestablishing that agencies are to implement agency-wide information security programs, establish a CIO position, report agency-specific cybersecurity incidents to Congress, and provide annual reports on the progress of implementing an information security program under FISMA 2014.[130] FISMA 2014 modified reporting requirements, mandating that agencies use automated tools and report more information related to cyber threats, security incidents, and compliance with FISMA 2014's

[126] 44 U.S.C. § 3541 (2012).
[127] *Is the OPM Data Breach the Tip of the Iceberg?*: *Hearing Before the Subcomm. On Research & Tech. and Oversight of the Comm. On Sci., Space, and Tech.,* 114th Cong. 4 (July 8, 2015).
[128] *See Federal Information Security Modernization Act (FISMA)*, U.S. DEPT. OF HOMELAND SECURITY, http://www.dhs.gov/fisma (last visited Oct. 16, 2015); S. REP. NO. 113-256, at 9-10 (2014).
[129] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-15-758T, INFORMATION SECURITY: CYBER THREATS AND DATA BREACHES ILLUSTRATE NEED FOR STRONGER CONTROLS ACROSS FEDERAL AGENCIES 3 (2015) [hereinafter GAO-15-758T].
[130] S. REP. NO. 113-256, at 10 (2014).

security requirements.[131] Additionally, FISMA 2014 required that the annual independent evaluations conducted by agency IGs include an assessment of the effectiveness of the agency's information security policies and practices, as opposed to just an assessment of agency compliance with FISMA requirements and OMB guidelines.[132] The law also required agencies to provide notice to Congress within seven days of a major cybersecurity incident, with OMB defining what constitutes a "major" incident.[133]

A significant change from FISMA 2002 to FISMA 2014 was codification of DHS' responsibilities as they relate to federal cybersecurity. FISMA 2014 authorized DHS to assist OMB in administering agency information security programs through the coordination of government-wide information security efforts, collaboration with NIST, and technical and operational assistance to other federal agencies.[134] Additionally, FISMA 2014 authorized DHS to issue binding operational directives to agencies in order to provide compulsory direction to agencies in the implementation of OMB policies, standards, and guidelines.[135] These directives include instructions for reporting security incidents, details on the type of information to be included in annual reports, and operational standards.[136] However, while FISMA 2014 authorized DHS to provide oversight of cybersecurity operations, it "[does] not authorize the department to take control of networks during emergencies."[137]

---

[131] Caitlin Meade & Susan Cassidy, *FISMA Updated and Modernized*, INSIDE GOV'T CONT. – PROCUREMENT AND POL'Y INSIGHTS (Dec. 19, 2014), http://www.inside governmentcontracts. com/2014/12/fisma-updated-and-modernized (providing a summary of the changes from FISMA 2002 to FISMA 2014).
[132] GAO-15-714, *supra* note 28, at 10-11.
[133] Stacey Banks, *The Federal Information Security Modernization Act of 2014*, TENABLE NETWORK SECURITY (Jan. 16, 2015), https://www.tenable.com/blog/the-federal-information-security-modernization-act-of-2014.
[134] Meade & Cassidy, *supra* note 131.
[135] *Id.*
[136] GAO-15-714, *supra* note 28, at 10.
[137] Aliya Sternstein, *Senators Want Homeland Security to be a Leading Cyberdefense Agency*, NAT'L J. (July 23, 2015), http://www.nationaljournal.com/s/71528/senators-want-homeland-security-be-leading-cyberdefense-agency.

While there has been limited operational time since the enactment of FISMA 2014 to determine the effectiveness of its modernization of FISMA 2002, the changes that Congress made do not address many of the weaknesses of FISMA 2002 (described in depth below). FISMA 2014 still lacked consistent metrics designed to measure the quality and effectiveness of information security programs, as well as an enforcement mechanism or resources to ensure agencies comply with standards and address deficiencies in their cybersecurity programs.

D. Challenges with FISMA

FISMA 2002, and its reformed FISMA 2014 (collectively henceforth, "FISMA"), provided a framework for the implementation of information security controls for federal agencies. However, as a legislative framework, FISMA has ultimately proved to be "too weak to effectively prevent cyber intrusions."[138] Agencies implementing information security programs directed at satisfying the reporting requirements under FISMA will not necessarily see the results in an effective information security program capable of protecting against cyber threats.[139] This is because FISMA establishes a framework to achieve a minimum acceptable level of security, permitting agencies the flexibility to simply satisfy FISMA's reporting requirements without actually implementing a risk management strategy to information security.[140] As a result, in recent years, agencies have experienced a significant increase in the overall number of security incidents, including a more than 1,120

[138] ROLLINS & HENNING, *supra* note 8, at 5.

[139] HOWARD, *supra* note 87, at 27 ("An information security program established and implemented to comply with FISMA can result in an effective program that meets an agency's risk-based needs for security. However, implementing security that aims to satisfy FISMA reporting requirements will not necessarily lead to an effective information security program."). *See also* William Jackson, *Homeland Security Tops FISMA Scorecard. How Do They Do It?*, GCN (June 19, 2014), https://gcn.com/articles/2014/06/19/dhs-oig-fisma-monitoring.aspx ("[C]ompliance does not equal security.").

[140] HOWARD, *supra* note 87, at 27.

percent increase from FY 2006 through FY 2014,[141] demonstrating that federal systems remain at risk and may not actually be more secure under FISMA.

FISMA is a "well-intentioned but fundamentally flawed tool" because it provides a mechanism for information security planning as opposed to serving as an effective method for actually measuring and improving information security.[142] A criticism of FISMA is that agencies and security officials often view the requirements as a "checklist" or "paperwork drill."[143] The assignment of annual letter grades to the 24 major agencies by the House Committee on Government Reform based on the annual FISMA reports has only perpetuated this.[144] Rather than incentivizing agencies to improve information security programs, this report card led agencies to adopt a "check the box" approach to meet FISMA's requirements in order to achieve a passing grade.[145]

Without a strong enforcing mechanism under FISMA, agencies lacked incentives to comply with the statute's requirements, and as such, implementation of cybersecurity programs under FISMA has not consistently occurred across government.[146] "An underlying cause for information security weaknesses . . . is that [agencies] have not yet fully or effectively implemented an agency wide information security program"[147] as required by FISMA. By the start of FY 2006, none of the 24 major agencies had implemented an agency-wide information security program,[148] and by the start of FY

---

[141] GAO-15-714, *supra* note 28, at 11. In FY 2014, the number of information security incidents that federal agencies reported was 67,168, a rise from 41,776 in FY 2010 and 5,503 in FY 2006. *Id.*; GAO-12-137, *supra* note 92, at 4.
[142] William Jackson, *FISMA's Effectiveness Questioned*, GCN (Mar. 18, 2007), https://gcn.com/Articles/2007/ 03/18/FISMAs-effectiveness-questioned.aspx.
[143] *Id.*
[144] *See* William Jackson, *FISMA Grades: What Do They Mean?*, GCN (Apr. 23, 2007), https:// gcn.com/articles/2007/04/23/fisma-grades-what-do-they-mean.aspx.
[145] HOWARD, *supra* note 87, at 30.
[146] *See, e.g.*, Silvers, *supra* note 15, at 1858; William Jackson, *Keith Rhodes: Effective IT Security Starts with Risk Analysis, Former GAO CTO Says*, GCN (June 10, 2009), https:// gcn.com/Articles/2009/06/15/Interview-Keith-Rhodes-IT-security.aspx.
[147] GAO-12-137, *supra* note 91, at 16.
[148] *No Computer System Left Behind: A Review of the 2005 Federal Computer Security Scorecards Before the H. Comm. on Gov't Reform*, 109th Cong. 32 (2006) (statement

2013, still none of the 24 major federal agencies had fully or effectively implemented the entire information security program components required under FISMA.[149] A fully implemented agency-wide information security program would provide the agency with a continuing cycle for assessing risk, developing security policies and procedures, facilitating awareness for information security, and establishing remediation activities to address deficiencies.[150] Failure to implement such a program could lead to inadequate protection of sensitive information.[151] "Until agencies fully resolve identified deficiencies in their agency wide information security programs, the federal government will continue to face significant challenges in protecting its information systems and networks."[152] As further evidence of the slow implementation of FISMA requirements, by the start of FY 2015, over a decade after the enactment of FISMA 2002, only 41 percent of non-Department of Defense agencies had implemented the "Strong Authentication" requirements, which requires agencies to provide employees with enhanced security credentials.[153]

In multiple U.S. Government Accountability Office ("GAO") reports issued since 2008, GAO has identified that, despite agency self-reported progress in implementing FISMA 2002's requirements, "major federal agencies continue to experience significant information security control deficiencies that limit the effectiveness of their efforts to protect the confidentiality, integrity, and availability of their information and information systems."[154]

---

of Gregory C. Wilshusen, Director, Information Security Issues, U.S. Government Accountability Office).

[149] *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-13-776, FEDERAL INFORMATION SECURITY: MIXED PROGRESS IN IMPLEMENTING PROGRAM COMPONENTS; IMPROVED METRICS NEEDED TO MEASURE EFFECTIVENESS 1, 44-45 (2013) [hereinafter GAO-13-776].

[150] GAO-08-571T, *supra* note 16, at 19.

[151] GAO-12-137, *supra* note 91, at 16.

[152] *Id.*

[153] OMB FY14 FISMA Report, *supra* note 99, at 6-7 (implementation of "Strong Authentication" requires users to log-on to federal networks with unique identification cards).

[154] GAO-08-571T, *supra* note 16, at 3. *See also* GAO-15-714, *supra* note 28, at 11; GAO-12-137, *supra* note 91, at 33.

Additionally, agencies have not adequately overseen the security requirements for information systems operated by federal contractors.[155] By FY 2008, nearly half of agency IGs reported that their agency did not consistently ensure that information systems used by contractors met FISMA requirements, NIST standards, or OMB policies,[156] and by FY 2012, 75 percent of agency IGs identified weaknesses in agency oversight of contractor information systems.[157] GAO concluded that federal systems and information are at an increased risk for unauthorized access to sensitive information, but that agencies could improve their cybersecurity posture by implementing the hundreds of recommendations made by IGs and GAO based on prior evaluations and identified weaknesses.[158]

In many situations, agencies were aware of their cybersecurity issues and information security program weaknesses, but they failed to take sufficient action.[159] For instance, many of the issues with OPM's information security programs were systemic, and OPM's IG had identified them as early as FY 2007.[160] In its FY 2014 annual audit report, the OPM IG summarized its findings based on its evaluation of OPM's information technology security program and practices, identifying material weaknesses related to the information security governance; material weaknesses in the internal control structure of OPM's IT security program; lack of a comprehensive inventory of servers, databases, and network devices; failure to adequately monitor its systems; and failure to adequately test its systems.[161] The IG also identified that, of OPM's 47 major information systems, 38 of these systems had known vulnerabilities

[155] GAO-12-137, *supra* note 91, at 32.
[156] *See* GAO-08-571T, *supra* note 16, at 10.
[157] GAO-12-137, *supra* note 91, at 32.
[158] GAO-08-571T, *supra* note 16, at 3.
[159] *See* GAO-15-714, *supra* note 28, at 11; GAO-12-137, *supra* note 91, at 27-28.
[160] *Is the OPM Data Breach the Tip of the Iceberg?: Hearing Before the Subcomm. on Research & Tech. and Oversight of the Comm. on Sci., Space, and Tech.,* 114th Cong. 3 (2015) (statement of Michael R. Esser, OPM Assistant IG for Audits).
[161] U.S. OFFICE OF PERS. MGMT., OFFICE OF THE INSPECTOR GEN., 4A-CI-00-14-016, FINAL AUDIT REPORT: FEDERAL INFORMATION SECURITY MANAGEMENT ACT AUDIT FY 2014 (2014).

that could potentially lead to data breaches.[162] As the IG stated, "even when [OPM] has known about security vulnerabilities, it has failed to take action."[163] Because of its findings, the IG provided OPM with 29 recommendations to address the information security weaknesses, many of which were recommendations that previous audit reports provided.[164] Ultimately, OPM's IG reported these weaknesses and OPM's failure to manage its information systems and infrastructure culminated in the cyber breaches in June 2015.[165] Even after these attacks, OPM's IG remains concerned that OPM's plans to address the material weaknesses in its information systems will still leave the agency's systems insufficiently protected against future attacks.[166]

Despite the repeated identification of weaknesses, as well as the countless opportunities for improvement, federal agencies are not held accountable for failing to comply with the requirements of FISMA or implementing the recommendations stemming from the annual evaluations of their federal information security programs. A review of OPM's implementation of FISMA demonstrates this lack of accountability associated with an agency's failure to meet FISMA's requirements and provides an example of the consequences that can result. "Too many federal agencies like OPM fail to meet the basic standards of cybersecurity, and no one is being held accountable."[167] The lack of accountability was in part due to the ineffective tools available to OMB to enforce the requirements, but also the decentralized structure for oversight responsibility.[168] Failure to hold

---

[162] *Is the OPM Data Breach the Tip of the Iceberg?, Hearing Before the Subcomm. on Research & Tech. and Oversight of the Comm. on Sci., Space, and Tech.,* 114th Cong. 7-8 (2015) (statement of Michael R. Esser, OPM Assistant IG for Audits).

[163] *Id.*

[164] *Id.* at 7.

[165] *Id.* at 2.

[166] U.S. OFFICE OF PERS. MGMT., OFFICE OF THE INSPECTOR GEN., 4A-CI-00-15-011, FINAL AUDIT REPORT: FEDERAL INFORMATION SECURITY MANAGEMENT ACT AUDIT FY 2015 (2015).

[167] Zach Noble, *Fixing FISMA, Blaming. . . Someone, and Another Lawsuit*, FCW: THE BUS. OF FED. TECH. (July 9, 2015), https://fcw.com/articles/2015/07/09/opm-breach-hearing.aspx (quoting Rep. Lamar Smith).

[168] *See, e.g.*, Silvers, *supra* note 15, at 1863 ("FISMA vests degrees of responsibility in at least four individuals within each agency: the agency head herself; the agency IG and CIO; and the agency's CIO's specially designated assistant for FISMA. This means that in any given agency at least four senior executives share FISMA oversight

agencies accountable for appropriately managing their information security programs and addressing long-standing cyber issues may lead to a continued increase in cyber attacks on federal systems.

E. Federal Information Security Management Reform Act

In the wake of the OPM cyber incidents, a bi-partisan group of legislators introduced FISMRA 2015, which sought to update FISMA 2014 by providing additional authority to DHS.[169]

> "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 [DHS] has the tools it needs to adequately secure our federal civilian networks."[170]

These members of Congress are concerned that, under the current legislation, DHS "does have the 'teeth' to actually enforce security standards or fix vulnerabilities."[171]

The proposed statute would allow DHS to monitor all agency systems using intrusion detection and prevention technology.[172] Under the FISMA 2014 framework, DHS needs permission from an agency in order to investigate or monitor that agency's systems.[173] Under the FISMRA 2015 proposals, DHS would have the authority to monitor agency systems without permission.[174] Using this authority, DHS would be able to conduct risk assessments, as well as

---

responsibility . . . This kind of overlapping and duplicative responsibility breeds the administrative inertia and complacency for which bureaucracies are (in)famous.").

[169] Jason Miller, *Senators Want DHS to Have NSA-Like Defensive Cyber Powers*, FED. NEWS RADIO (July 23, 2015), http://federalnewsradio.com/legislation/2015/07/senators-want-dhs-nsa-like-defensive-cyber-powers.

[170] Sternstein, *supra* note 137 (quoting Sen. Mark Warner) (internal quotation marks omitted).

[171] 161 CONG. REC. S5456 (daily ed. July 22, 2015) (statement of Sen. Warner).

[172] Sternstein, *supra* note 137.

[173] Cory Bennett, *Senators Unveil New Homeland Security Cyber Bill*, THE HILL (July 22, 2015), http://thehill.com/policy/cybersecurity/248775-senators-set-to-unveil-new-dhs-cyber-bill.

[174] *Id.*

scan for and repel attacks, of any network within the dot-gov domain.[175] If DHS detects a threat, they would have the power to direct agencies "to take any lawful action with respect to the operation of the information system at risk."[176]

Under this reform, DHS would have a more significant and military-like role in federal cybersecurity with the authority to intervene and monitor other agencies' information systems and conduct defensive countermeasures to improve cybersecurity.[177] While FISMRA 2015 would take additional steps to protect the federal information infrastructure through increased threat detection and provides a stronger enforcing function via DHS, there are concerns that DHS may not have the capability to satisfy the bill's requirements.[178] Further, the proposed legislation does not address the lack of meaningful metrics designed to measure the effectiveness of information security programs, nor does it provide DHS with sufficient tools to ensure agency compliance with cybersecurity standards.

F. Role of the Executive Branch in Cybersecurity

The Constitution grants the executive and legislative branches authority relating to national security.[179] However, there is some disagreement as to whether the White House has supreme authority and oversight for cybersecurity,[180] or whether this authority is limited to responsibility for cybersecurity emergencies only.[181] Regardless of which branch of government should "own" cybersecurity regulation and enforcement, the executive branch has recently taken more action to address cybersecurity issues because of

---

[175] *See* Miller, *supra* note 169; Sternstein, *supra* note 137 (internal quotation marks omitted).
[176] Sternstein, *supra* note 137.
[177] *See* Miller, *supra* note 169.
[178] *See id.*
[179] ROLLINS & HENNING, *supra* note 8, at 10.
[180] *Id.* at 5 (quoting *Cybersecurity Recommendations for the Next Administration: Hearing Before the Subcomm. on Emerging Threats, Cybersecurity and Sci. and Tech. of the H. Homeland Sec. Comm.*, 110th CONG. 19 (Sept. 16, 2008)).
[181] *See* Fredland, *supra* note 42, at 10.

inaction by Congress and disagreements between these branches and relevant stakeholders about the appropriate action.[182]

In February 2013, President Obama signed Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, in response to repeated cyber attacks of critical infrastructure.[183] This Executive Order had two primary focuses: "cybersecurity information sharing and the development and implementation of risk-based cybersecurity standards for critical infrastructure."[184] It specifically ordered the NIST to lead the development of a cybersecurity framework to reduce cybersecurity risks to critical infrastructure, and it directed the Secretary of Homeland Security to set performance goals within this framework.[185]

The President issued Executive Order 13636 in part due to Congress' inaction and failure to enact cybersecurity legislation.[186] Through this Executive Order, "the White House focused its efforts on critical infrastructure protection, the most controversial part of the comprehensive cybersecurity legislation that failed in the Senate."[187] But critics argued that an Executive Order of this nature was not strong enough to address the issues and only legislation, enacted through the democratic process, would effectively impact the

---

[182] Ferraro, *supra* note 11, at 300 ("The executive branch has taken action to address cybersecurity, recently through an Executive order meant to strengthen public-private cooperation on electronic infrastructure protection, but broader legislation intended to bolster cybersecurity has failed due to disagreements among the U.S. House, Senate, and White House, and privacy advocates, business interests, and security specialists.").

[183] Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 12, 2013).

[184] Teplinsky, *supra* note 28, at 297.

[185] ERIC A. FISCHER ET AL., CONG. RESEARCH SERV., R42984, THE 2013 CYBERSECURITY EXECUTIVE ORDER: OVERVIEW AND CONSIDERATIONS FOR CONGRESS 8-9 (2014).

[186] *Id.* at 14 ("E.O. 13636 was issued in the wake of the lack of enactment of cybersecurity legislation in the 112th Congress, apparently at least in part as a response to that."). *See also* Ferraro, *supra* note 11, at 300 ("The executive branch has taken action to address cybersecurity, recently through an Executive order meant to strengthen public-private cooperation on electronic infrastructure protection, but broader legislation intended to bolster cybersecurity has failed due to disagreements among the U.S. House, Senate, and White House, and privacy advocates, business interests, and security specialists.").

[187] Teplinsky, *supra* note 28, at 295.

nation's cybersecurity posture.[188] At the very least, this Order was an early step by the executive branch in addressing the nation's cybersecurity challenges.[189]

Nearly two years later, President Obama issued Executive Order 13691, *Promoting Private Cybersecurity Information Sharing*, to encourage private entities to share information related to cybersecurity risks and incidents across the private sector and with the government, with the goal of increasing collaboration to develop mechanisms to improve cybersecurity capabilities and protections.[190] This Executive Order does not impose mandatory requirements on private corporations; rather, it establishes a framework for voluntary information sharing and creates protections from public disclosure to encourage sharing among these entities.[191] As a result, DHS is working to establish best practices for information sharing to aid private corporations in sharing information with each other and the government.[192] But again, this Order is just one step in addressing cybersecurity and, specifically, the sharing of cyber threats, an area where little legislative action has occurred to date.[193]

---

[188] John McCain et al., *No Cybersecurity Executive Order, Please*, WALL ST. J., Sept. 14, 2012, at A13.
[189] *See* J. Nicholas Hoover, *Cybersecurity Executive Order Leaves Tough Work Undone*, INFO. WEEK (Feb. 13, 2013), http://www.darkreading.com/risk-management/cybersecurity-executive-order-leaves-tough-work-undone.
[190] Exec. Order No. 13,691, 80 Fed. Reg. 9,349 (Feb. 13, 2015).
[191] *See* WHITE HOUSE: OFFICE OF THE PRESS SEC'Y, FACT SHEET: EXECUTIVE ORDER PROMOTING PRIVATE SECTOR CYBERSECURITY INFORMATION (Feb. 12, 2015).
[192] *Jeh Johnson on U.S. Cybersecurity Readiness*, COUNCIL ON FOREIGN REL. (Nov. 4, 2015), http://www.cfr.org/homeland-security/jeh-johnson-us-cybersecurity-readiness/p37196 (providing a transcript of a conversation between Jeh Johnson, DHS Secretary, and Andrea Mitchell, Chief Foreign Affairs Correspondent for NBC News, conducted during a Council on Foreign Relations Cybersecurity Symposium).
[193] Ron Gula, *Opinion: Why the "Cyber Bill" Falls Short on Protecting Critical Networks*, THE CHRISTIAN SCI. MONITOR (Oct. 21, 2015), http://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/1021/Opinion-Why-the-cyber-bill-falls-short-on-protecting-critical-networks.

IV. RECOMMENDATIONS FOR A FEDERAL CYBERSECURITY LEGISLATIVE FRAMEWORK

This section provides recommendations for modifying the United States federal cybersecurity legislative framework, which includes addressing the challenges identified with current legislation and proposed legislation aimed at regulating federal systems to better guard against cyber threats and improve the protection of the federal information infrastructure. Specifically, this section addresses the need for the legislative framework to be revised to establish meaningful standards for federal information security programs, identification of an enforcement mechanism, as well as the need to ensure federal agencies have the appropriate resources to address cybersecurity weaknesses.

A. Standards: Need for a Clear Framework that Improves Information Systems through Meaningful Metrics and an Accountable Official

Framework legislation for cybersecurity is beneficial in that it provides an overall structure and process within which agencies can operate to address complicated cyber issues.[194] Congress should require definition and enhancement of the standards for agency compliance within the current legislative framework for federal information security to ensure standards are meaningful.[195] "The current metrics do not measure how effectively agencies are performing various activities."[196] As GAO described, agencies must currently test the effectiveness of the security controls of their information systems and include information on the number of systems undergoing these tests in their annual reports, but there is no consistent standard associated with the quality of the tests being conducted across government.[197] Thus, information security metrics associated with FISMA must be modified to be clear and measurable against established performance targets to allow monitoring of progress over time, and they must focus on the quality of agency

[194] *See* Delaney, *supra* note 10, at 267-68.
[195] *See* GAO-12-137, *supra* note 91, at 21.
[196] GAO-08-571T, *supra* note 16, at 27.
[197] *Id.*

performance in implementing security controls and managing risk to their information systems.

However, advances in technology could outpace the government's ability to define and update standards for enforcement. Therefore, OMB and NIST will need to continuously assess and revise these standards against current and emerging cybersecurity risks and threats to ensure they do not become obsolete.[198]

OMB should also clarify how the independent IGs evaluations of agency information security programs are conducted. Currently, there is no common approach or methodology, and thus, IG evaluations vary across agencies.[199] Reporting guidance has been incomplete, and IG responses to the evaluation have been inconsistent as a result.[200] These independent evaluations can serve as an effective method for determining agency compliance with established guidelines and metrics, but consistency in the assessment process and quality control must exist first.

Establishing new standards, or enhancing existing metrics, are not sufficient; these standards must be enforced and agencies must be held accountable for non-compliance. Annual IG evaluations, as well as external organization assessments such as the GAO, have consistently identified weaknesses and provided hundreds of recommendations for improvement,[201] but agencies have been slow to act, in part because of a lack of an enforcement mechanism.

To ensure proper accountability and enforcement across government, cybersecurity legislation should establish a senior accountable official that serves as the individual responsible for ensuring implementation of federal information security requirements. This individual, and supporting resources consisting

---

[198] Gable, *supra* note 30, at 98 ("[I]f better standards and security measures are not continually developed, those working to break security mechanisms will quickly catch up to and surpass those trying to maintain security.").
[199] GAO-08-571T, *supra* note 16, at 28.
[200] *See* GAO-15-714, *supra* note 28, at 52.
[201] *See* GAO-08-571T, *supra* note 16, at 3.

of information security business experts, should reside in OMB to demonstrate the importance of securing and sustaining effective federal systems. When agencies do not comply with established standards or fail to address significant information security program deficiencies, this cyber-accountability official would have the authority to assemble a team of experts from its own office and across government to work directly with the struggling agency to build the necessary framework in an expedient manner. This cyber-accountability official must have the authority to inspect agency information systems and information security programs at any time and without advanced notice. If an agency fails to comply or cooperate, this responsible entity would have the power to enforce sanctions to hold the agency accountable and incentivize action.[202] This provides a "carrot and the stick" approach, with the carrot being assistance to the agency and the stick being sanctions. A cyber-accountability official has the benefit of ensuring uniformity and consistency in the implementation of established standards and allows for identification of lessons learned and the application of best practices across government. At the end of the day, agencies must have the proper incentive to act before another OPM-like incident—or worse—occurs.

B. Resources: Need for Greater Flexibility to Hire Cyber Talent and Consistent Funding for Cybersecurity

But standards, and an individual to enforce these standards, may be insufficient. Federal agencies must have the appropriate resources, both human capital and financial, to develop and sustain effective information security programs to protect the current federal information infrastructure and guard against complex and emerging cyber threats.[203] Without sufficient resources in place to achieve identified targets, information security standards are meaningless.

---

[202] Silvers, *supra* note 15, at 1869 ("Surprise inspections have an established pedigree within the federal administrative state. They have been used successfully in several regulatory contexts as a means of enhancing compliance 'by increasing the likelihood that violations will be detected.'").

[203] *See, e.g.*, Gula, *supra* note 193 ("Success may mean hiring more cybersecurity experts, and/or investing in tools to detect and remediate network vulnerabilities

Government agencies need to be able to recruit and retain a high caliber workforce with the expertise and capabilities necessary to implement and maintain effective information security programs. As the federal government is responsible for protecting its critical information infrastructure and the sensitive information that resides within its networks, it must have the cybersecurity talent in place to accomplish this. However, federal agencies have historically struggled to recruit, hire, retain, and train skilled workers in information technology and cybersecurity fields.[204] "There is a nationwide shortage of highly qualified cybersecurity experts, and the federal government in particular has fallen behind in the race for this talent."[205] This is in part because the federal government lacks a comprehensive or coordinated strategy to recruit and retain a skilled cyber workforce,[206] and many agencies, particularly those with smaller cybersecurity programs, have difficulty recruiting the right talents.[207] The government must establish a comprehensive strategy to address its cybersecurity needs and deficiencies, in alignment with the legislative requirements under FISMA. In turn, reforms to cybersecurity legislation must provide federal agencies with flexibilities to break from the antiquated federal hiring and personnel system through expedited hiring[208] and advanced, market-sensitive compensation to attract and retain the right cyber talent.

Without proper funding, agencies will not be able to support implementation of effective information security programs. Requiring agencies to perform additional work without additional

with fewer personnel. The security industry is experiencing a severe talent drought, so competition for top performers is intense. At the same time, good tools cost money; however the return for the right tool is often worth the initial cost.").

[204] P'SHIP FOR PUB. SERV., CYBER IN-SECURITY II: CLOSING THE FEDERAL TALENT GAP 1 (2015) [hereinafter P'SHIP FOR PUB. SERV., CYBER IN-SECURITY II]; *see also* P'SHIP FOR PUB. SERV., CYBER IN-SECURITY I: STRENGTHENING THE FEDERAL CYBERSECURITY WORKFORCE 1 (2009) [hereinafter P'SHIP FOR PUB. SERV., CYBER IN-SECURITY I].

[205] P'SHIP FOR PUB. SERV., CYBER IN-SECURITY II, *supra* note 204, at 1.

[206] *See id.* at 2.

[207] *See* P'SHIP FOR PUB. SERV., CYBER IN-SECURITY I, *supra* note 204, at 8.

[208] While direct hire authority exists to allow for an expedited hiring process when there is a critical hiring need or severe shortage of qualified candidates, this authority only exists for certain cybersecurity subspecialties and use has been limited. P'SHIP FOR PUB. SERV., CYBER IN-SECURITY II, *supra* note 204, at 14-16.

funds is unlikely to result in compliance with the statute. This was demonstrated after the enactment of FISMA 2002.[209] Specifically, agency heads were required to ensure adequate staffing of trained personnel to support FISMA requirements;[210] however, agencies lacked additional funds for these staffs or other resources to implement FISMA requirements and were expected to improve their cybersecurity posture within the constraints of preexisting budgets.[211]

The amount that agencies spend on information security fluctuates from year to year. From FY 2010 through FY 2014, the 24 major agencies total spending on cybersecurity varied between 10.3 billion dollars (FY 2013) and 14.6 billion dollars (FY 2012),[212] with nearly two-thirds of this dedicated to the Department of Defense.[213] Funding provided to individual agencies for cybersecurity also varies, with factors such as the recent occurrence of a major cyber incident potentially playing a role in that determination. For instance, following the OPM cyber incidents in 2015, OPM received a significant funding increase in FY 2016 compared to FY 2015, which included 21 million dollars (or approximately eight percent of its total budget) devoted to cybersecurity.[214] For comparison, OPM previously spent nearly the lowest amount in federal government on cybersecurity, spending only seven million dollars in FY 2014.[215]

---

[209] Silvers, *supra* note 15, at 1859 ("FISMA does not directly bring new funding to the agencies. So, while agencies must perform more work-often with the assistance of costly private contractors-they must effectively do so within the constraints of their preexisting budgets. For bureaus that already consider themselves strapped for cash, these new tasks may foster reluctance towards implementation, and perhaps even resentment aimed at those ordering the new work to be performed.").

[210] HOWARD, *supra* note 87, at 17.

[211] Silvers, *supra* note 15, at 1859; *see also* HOWARD, *supra* note 87, at 31 ("Agencies were not given additional funding to meet FISMA requirements, but had to reprogram from existing funding to meet the additional information security requirements.").

[212] GAO-15-714, *supra* note 28, at 46.

[213] Gula, *supra* note 193.

[214] Eric Katz, *Winners and Losers in the Omnibus Spending Bill*, GOV'T EXEC. (Dec. 17, 2015), http://www.govexec.com/management/2015/12/winners-and-losers-omnibus-spending-bill/124600.

[215] Mohana Ravindranath, *Before Breach, OPM Requested Millions of Dollars to Upgrade Network Security*, NEXTGOV (June 5, 2015), http://www.nextgov.com/cybersecurity/2015/06/ breach-opm-requested-32-million-more-cyber/114580.

While the 21 million dollars for cybersecurity at OPM was requested by the agency before the announcement of the recent cyber incidents in June 2015, it is evident that an increase in funding is required for this agency to implement network and information technology infrastructure upgrades and ensure an effective information security program.[216]

"Simply spending more money doesn't automatically make you more secure, but if the U.S. government wants to keep the nation secure and protect America's private data, it must invest more in cybersecurity."[217] Therefore, Congress and OMB should assess the allocation of funds to federal agencies to determine appropriate levels of funding necessary to resolve systemic information security issues and develop information security programs that are capable of responding to complex and emerging cyber threats.

Recognizing that providing agencies with an infinite amount of resources to establish premier information security programs or address long-standing deficiencies in cybersecurity would be impossible, cost-sharing steps should be taken where practicable. Therefore, the use of government-wide activities and common practices should be evaluated to identify areas within the information security realm for cost sharing or use of shared services among federal agencies.

V. CONCLUSION

The United States is unable to adequately protect against the increasingly frequent and sophisticated cyber threats to federal information infrastructures because the nation lacks an effective cybersecurity legislative framework for the regulation of government systems. While FISMA 2002, and its reform in FISMA 2014, provides a framework, it is limited and ineffective at ensuring government agencies adhere to the requirements established by existing statutes. As a result, government entities remain at unnecessary risk and are becoming increasingly susceptible to cyber

[216] *See* U.S. OFFICE OF PERS. MGMT, FY 2016 CONGRESSIONAL BUDGET JUSTIFICATION 2 (2015).
[217] Gula, *supra* note 193.

attack. "It is not a matter of if, but of when government systems will again be hit by a major cyber attack,"[218] and it is critical to our national security that Congress take immediate steps to enact legislation that effectively regulates the cybersecurity of federal systems. Reforms to legislation related to federal cybersecurity must establish a clear, meaningful regulatory framework that includes specific, measurable standards for federal agencies to implement and provides a means for ensuring accountability. Federal agencies must be given appropriate resources—people and dollars—to address systemic cybersecurity weaknesses and develop effective information security programs. Failing to improve the U.S. cybersecurity regulatory framework to ensure adequate protection of federal systems will inevitably result in future cyber attacks of a debilitating nature.

[218] 161 CONG. REC. S5456 (daily ed. July 22, 2015) (statement of Sen. Warner).