CYBERSECURITY: WHAT ABOUT U.S. POLICY?

Lawrence J. Trautman†

This article is inspired by the potential of significant new university initiatives on cybersecurity research: First, at the Harvard Berkman Center for Internet and Society's forthcoming project on Cybersecurity: Rethinking the Role of the Foreign Intelligence Community in Promoting Cybersecurity. Thanks to Jonathan Zittrain (Principal Investigator), Matt Olsen, Bruce Schneier, Urs Gasser, David O'Brien, and Rob Faris for undertaking this important project. Next, a recent gift by the William and Flora Hewlett Foundation has resulted in the establishment of three major new cybersecurity policy research initiatives at: the Massachusetts Institute of Technology (MIT); Stanford University; and University of California, Berkeley. Also deserving special mention is Southern Methodist University's Darwin Deason Institute for Cyber Security. Particular thanks to Frederick R. Chang, Carol Mullins Hayes, Admiral Bobby R. Inman, USN (Retired), Mitchell Kominsky, Stuart S. Malawer, and Julie J.C.H. Ryan for their assistance in the research and preparation of this article. All errors and omissions are my own.

Abstract

During December 2014, just hours before the holiday recess, the U.S. Congress passed five major legislative proposals designed to enhance U.S. cybersecurity. Following signature by the President, these became the first cybersecurity laws to be enacted in over a decade, since passage of the Federal Information Security Management Act of 2002. My goal is to explore the unusually complex subject of cybersecurity policy in a highly readable manner. An analogy with the recent deadly and global Ebola epidemic is used to illustrate policy challenges, and hopefully will assist in transforming the technological language of cybersecurity into a more easily understandable story. Much like Ebola, cyberthreat has the ability to bring our cities to a standstill. Many cybersecurity policy implications are strikingly similar to those occasioned by Ebola.

First, a brief recital of the grave danger and potential consequences of

† BA, The American University; MBA, The George Washington University; post-graduate studies (Management Information Systems) University of Texas at Dallas; and JD, Oklahoma City Univ. School of Law. Mr. Trautman is a past president of the Dallas Internet Society and the New York and Metropolitan Washington/Baltimore Chapters of the National Association of Corporate Directors. He may be reached at Lawrence.J.Trautman@gmail.com.

cyberattack is provided. Second, I comment on the policy impact resulting from rapid changes in technological complexity and the relative lack of computer familiarity on the part of many senior business and governmental leaders. Third, the characteristics of selected competing cybersecurity constituency groups are discussed: consumers; investors; law enforcement; business; federal, state and local government; and national security interests. By exploring the perceived needs and sometimes conflicting actions of these various constituencies, I hope to make a worthwhile contribution to the national conversation about cyber policy and make meaningful progress toward dealing with the new pandemic of technological virus. Next, is an examination of recent policy development milestones achieved during the past decade or so, including passage of several major legislative proposals designed to enhance U.S. cybersecurity during the waning hours of 2014: The National Cybersecurity Protection Act of 2014; The Federal Information Security Modernization Act of 2014; The Cybersecurity Workforce Assessment Act; The Homeland Security Workforce Assessment Act; and The Cybersecurity Enhancement Act of 2014. Finally, given the critical need for an immediate and effective coordinated approach to cybersecurity, a few thoughts about crafting policy goals and strategies are offered. Hopefully this essay will assist in the conversation being had today by policy makers on this important topic.

TABLE OF CONTENTS

CYBERSECURITY: WHAT ABOUT U.S. POLICY?

> Our most pressing need is clear policy, formed by shared consensus, shaped by informed discussion, and created by a *common* body of knowledge. With no common knowledge, no meaningful discussion, and no consensus . . . the policy vacuum continues. This will not be easy . . . it will require courage; but, it is essential and should itself be the subject of intense discussion.[1]
>
> Gen Michael V. Hayden, USAF, Retired
> *Former Director, National Security Agency*
> *Former Director, Central Intelligence Agency*

1. Michael V. Hayden, *The Future of Things "Cyber,"* STRATEGIC STUD. Q., Spring 2011 at 3, 5.

I. OVERVIEW

During December 2014, just hours before the holiday recess, the U.S. Congress passed five major legislative proposals designed to enhance U.S. cybersecurity.[2] Following signature by the President, these became the first cybersecurity laws to be enacted in over a decade, since passage of the Federal Information Security Management Act of 2002.[3] Commander of U.S. Cyber Command and Director of the National Security Agency (NSA) Admiral Mike Rogers characterizes cyber attacks "as the greatest long-term threat to national security in part because 'we have yet to come to a broad policy and legal consensus.'"[4] Jonathan Zittrain of Harvard's Berkman Center for Internet and Society observes that "coordinated responses and comprehensive strategies to deal with mounting cybersecurity challenges have been understandably slow to develop."[5]

Accordingly, now is a good time to ask, "Where is U.S. Cybersecurity Policy?" Federal government agencies, particularly the SEC, require private companies to disclose potential cyber risks they experience during their everyday operations. Are some of our government agencies that administer well-intentioned cyber policy working at cross purposes? Any such *de novo* analysis of public policy calls for an examination of the various constituencies for cybersecurity and how their perceived needs fit into the aggregate societal good. Often, a major consideration in crafting cybersecurity policy requires policy makers and legislators to sort out the aggregate societal cost of various policy alternatives with highly imperfect information. Further complicating any cybersecurity policy analysis is the inconvenient fact that national security considerations, of necessity, will defy transparency of perceived risk, nature of the risk, and sources and methods of waging a defense to cyber threats.

---

2. *See generally* National Cybersecurity Protection Act of 2014, Pub. L. No. 113-282 (2014), https://www.congress.gov/bill/113th-congress/senate-bill/2519 (discussing the National Cybersecurity Protection Act of 2014's amendments to the Homeland Security Act of 2002); Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283 (2014), https://www.congress.gov/bill/113th-congress/senate-bill/2521 (discussing the Federal Information Security Modernization Act of 2014's amendments to the Federal Information Security Management Act of 2002) (requiring the Department of Homeland Security to create a strategy for cybersecurity); Cybersecurity Workforce Assessment Act, Pub. L. No. 113-246 (2014), https://www.congress.gov/bill/113th-congress/house-bill/2952/text; Border Patrol Agent Pay Reform Act of 2014, Pub. L. No: 113-277, https://www.congress.gov/bill/113th-congress/senate-bill/1691 (discussing the Cybersecurity Workforce Assessment Act); Cybersecurity Enhancement Act, Pub. L. No. 113-274 (2014), https://www.congress.gov/bill/113th-congress/senate-bill/1353 (citing various laws passed December 2014).

3. Mitchell S. Kominsky, *The Current Landscape of Cybersecurity Policy: Legislative Issues in the 113th Congress*, HARV. NAT'L SEC. J. (Feb. 6, 2014), http://harvardnsj.org/2014/02/the-current-landscape-of-cybersecurity-policy-legislative-issues-in-the-113th-congress [hereinafter Mitchell] (citing Eric A. Fischer, *Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions*, CONG. RES. SERV. (June 20, 2013), https://www.fas.org/sgp/crs/natsec/R42114.pdf).

4. Scott Shackelford & Andraz Kastelic, *Toward a State-Centric Cyber Peace? Analyzing the Role of National Cybersecurity Strategies in Enhancing Global Cybersecurity*, N.Y.U. J. OF LEGIS. AND PUB. POL'Y 1, 3 (2014), http://ssrn.com/abstract=2531733.

5. E-mail from Jonathan Zittrain, George Bemis Professor of Law at Harvard Law School and the Harvard Kennedy School of Government, Professor of Computer Sci. at the Harvard School of Eng'g and Applied Sciences, Vice Dean for Library and Info. Resources at the Harvard Law School Library, co-founder of the Berkman Center for Internet & Society, and Principal Investigator for the Harvard Cybersecurity Project to Lawrence J. Trautman (Dec. 12, 2014, 15:40 CST) (on file with author).

My goal is to explore the unusually complex subject of cybersecurity policy in a highly readable manner. An analogy with the recent deadly and global Ebola epidemic is used to illustrate policy challenges, and hopefully will assist in transforming the technological language of cybersecurity into a more easily understandable story. Much like Ebola, the technical mechanics of cyberthreat are not widely understood by the population at large. And, much like Ebola, cyberthreat has the ability to bring our cities to a standstill. Many cybersecurity policy implications are strikingly similar to those occasioned by Ebola.

First, a brief recital of the grave danger and potential consequences of cyberattack is presented. Second, I comment on the policy impact resulting from rapid changes in technological complexity and the relative lack of computer familiarity on the part of many senior business and governmental leaders. Third, the characteristics of selected competing cybersecurity constituency groups are discussed: consumers; investors; law enforcement; business; federal, state and local government; and national security interests. By exploring the perceived needs and sometimes conflicting actions of these various constituencies, I hope to make a worthwhile contribution to the national conversation about cyber policy and make meaningful progress toward dealing with the new pandemic of technological virus. Next, is an examination of recent policy development milestones achieved during the past decade or so, including passage of several major legislative proposals designed to enhance U.S. cybersecurity during the waning hours of 2014: The National Cybersecurity Protection Act of 2014;[6] The Federal Information Security Modernization Act of 2014;[7] The Cybersecurity Workforce Assessment Act;[8] The Homeland Security Workforce Assessment Act;[9] and The Cybersecurity Enhancement Act of 2014.[10] Finally, given the critical need for an immediate and effective coordinated approach to cybersecurity, a few thoughts about crafting policy goals and strategies are offered. Hopefully this essay will assist the conversation being had today by policy makers on this important topic.

II. CLEAR AND PRESENT DANGER

Reports of nation states mounting massive attacks against American computers are legion.[11] Mike McConnell, Booz Allen Hamilton Vice

6. National Cybersecurity Protection Act of 2014, Pub. L. No. 113-282 (2014), https://www.congress.gov/ bill/113th-congress/senate-bill/2519.

7. Federal Information Security Modernization Act of 2014, Pub. L. No: 113-283 (2014), https://www.congress.gov/bill/113th-congress/senate-bill/2521.

8. Cybersecurity Workforce Assessment Act, Pub. L. No: 113-246 (2014), https://www.congress.gov/bill/113th-congress/house-bill/2952/text.

9. Border Patrol Agent Pay Reform Act of 2014, Pub. L. No: 113-277 (2104), https://www.congress.gov/ bill/113th-congress/senate-bill/1691.

10. Cybersecurity Enhancement Act, Pub. L. No. 113-274 (2014), https://www.congress.gov/bill/113th-congress/senate-bill/1353.

11. The following provides examples of cyber attacks against American computers. *E.g.*, William J. Lynn, *Defending a New Domain*, 89 FOREIGN AFF. 97 (2010); *Communist Chinese Cyber-Attacks, Cyber-Espionage and Theft of American Technology: Hearing Before the H. Subcomm. on Oversight and Investigations of the Comm. on Foreign Affairs*, 112th Cong. 112–14 (2011); Nathan Alexander Sales,

Chairman and former U.S. Director of National Intelligence observes that "there isn't a corporation in the nation today that can't be penetrated, not one."[12] In prior Congressional testimony, Frederick Chang states, "Today our opponents in cyberspace are intelligent, seam-seeking, shape-shifting adversaries, that have an uncanny ability to penetrate and evade cyber defenses and compromise the targeted system."[13] Speaking at the 2014 New York Stock Exchange "Cyber Risks and the Boardroom" Conference, SEC Commissioner Luis A. Aguilar states that "over just a relatively short period of time, cybersecurity has become a top concern of American companies, financial institutions, law enforcement, and many regulators."[14] Senator Joseph Lieberman stated, "[t]he current ongoing and growing cyber threat not only threatens our security here at home, but it is right now having a very damaging impact on our economic prosperity."[15] The aggregate cost to the United States for cybersecurity defense and loss is incalculable. The full extent of intellectual property losses due to systems breaches will never be known with accuracy. One estimate is that the cost of cybercrime in the United States approximates $100 billion annually.[16] In their daily lives,

---

Regulating Cyber-Security, 107 NW. U.L. REV. 1503 (2013); Scott Shackelford & Amanda Craig, *Beyond the New "Digital Divide": Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity*, 50 STAN. J. INT'L L. 119 (2014); Annual Meeting Paper from Robert Axelrod, *The Strategic Timing of Cyber Exploits*, to American Political Science Association (Aug. 29–Sept. 1, 2013); Peter P. Swire, *A Model for When Disclosure Helps Security: What is Different About Computer and Network Security?*, 2 J. TELECOMM. & HIGH TECH. L. 163 (2004); Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue & Julia Spiegel, *The Law of Cyber-Attack*, 100 CAL. L. REV. 817 (2012); Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks*, 88 TEX. L. REV. 1533 (2010); Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429 (2012).

12. Ben Worthen, *Watching and Waiting*, WALL ST. J., Apr. 2, 2012, at R7.

13. *Is Your Data on the Healthcare.gov Website Secure?: Hearing Before the H. Committee on Sci., Space & Tech., Subcomm. on Tech. and the Subcomm. on Res.*, 113th Cong. (2013) (statement of Frederick R. Chang, Bobby B. Lyle Centennial Distinguished Chair in Cyber Security, Southern Methodist University).

14. Luis A. Aguilar, Comm'r, U.S. Sec. and Exch. Comm'n, Boards of Directors, Address Before the New York Stock Exchange, "Cyber Risks and the Boardroom" Conference: Corporate Governance and Cyber Risks: Sharpening the Focus (June 10, 2014) (transcript available on U.S. Sec. and Exchange Commission Website) http://www.sec.gov/News/Speech/Detail/Speech/1370542057946#.U6t-wvldWHg; *see Hearing on Homeland Threats and Agency Responses Before the S. Comm. on Homeland Sec. and Governmental Affairs*, 113th Cong. 4 (2013) (statement of James B. Comey Jr., Director, Federal Bureau of Investigation, U.S. Department of Justice) http://www.hsgac.senate.gov/hearings/threats-to-the-homeland ("[R]esources devoted to cyber-based threats will equal or even eclipse the resources devoted to non-cyber based terrorist threats."). See also, *Hearing on the Secretary's Vision for the Future—Challenges and Priorities Before the H. Comm. on Homeland Sec.*, 113th Cong. 7 (2014) (statement of Jeh C. Johnson, Secretary, U.S. Department of Homeland Security) ("DHS must continue efforts to address the growing cyber threat to the private sector and the dot-gov networks, illustrated by the real, pervasive, and ongoing series of attacks on public and private infrastructure.").

15. *Securing America's Future: The Cybersecurity Act of 2012: Hearing Before the Comm. on Homeland Sec. and Governmental Affairs*, 112th Cong. 1 (2012) (Opening Statement of Chairman Joseph Lieberman), http://www.hsgac.senate.gov/hearings/securing-americas-future-the-cybersecurity-act-of-2012. *See generally* Lawrence Trautman, *Virtual Currencies; Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox?*, 20 RICH. J.L. & TECH. 13, 15 (2014) http://ssrn.com/abstract=2393537 [hereinafter Bitcoin] (discussing the regulation of virtual currencies). *But see* Susan W. Brenner, *Cyber-Threats and the Limits of Bureaucratic Control*, MINN. J. L. SCI. & TECH 137 (2013), http://ssrn.com/abstract=1950725 (suggesting alternative methods of virtual currency regulation).

16. *See* Kominsky, *supra* note 3, *citing* Siobhan Gorman, *Annual U.S. Cybercrime Costs Estimated at $100 Billion*, WALL ST. J. (July 22, 2014), http://online.wsj.com/news/articles/SB10001424127887324328904578621880966242990.

Americans are finding that "cyberspace is vulnerable to an ever-evolving range of threats," according to Secretary of Homeland Security Jeh C. Johnson.[17] Secretary Johnson further observes that this vulnerability stems "from criminals to nation-state actors, ranging in purpose from identity and data theft to espionage and disruption of critical functions. As our Nation's reliance on cyber networks has grown, incidents which impact the safety and confidence with which we operate online have become increasingly commonplace."[18] Don't believe for a moment that the 2014 Ebola threat was just a flash in the pan event. While the influenza virus may have been with us since the beginning of time, according to many historians the first recognized case of pandemic influenza seems to be 500 years ago, in year 1510 A.D.[19] Laurence Barton reports that, "there have been ten pandemics over the past three centuries, the most notorious being the global flu of 1918 that killed tens of millions of people."[20] Barton continues,

> If you fast-forward to 1976, over 400 people died near the banks of the Ebola River in the Democratic Republic of the Congo as a result of a vicious, toxic pathogen. While 400 people may seem pithy compared to the death toll in 1918, it was the *manner* in which the victims of the Ebola virus died that should make you lose sleep; some medical journals reported that the organs of some of the victims poured out of their bodies within days of contracting the virus. Some in the medical community are concerned that if such a virus were to spread again (it had a whopping 95% fatality rate), the impact could be unprecedented. If local officials had not immediately burned affected bodies after the initial outbreak, some scientists have concluded that it was theoretically possible that the human race could have been obliterated within three months. This is no exaggeration: It was *that bad.*[21]

"The next Pearl Harbor that we confront could very well be a cyberattack that cripples America's electrical grid and its security and financial systems," observes Central Intelligence Agency Director Leon Panetta in his June 9, 2011 confirmation hearing for the post of secretary of defense before the Senate Armed Services Committee.[22] In testimony before the U.S. House Intelligence Committee, NSA Director Admiral Michael Rogers warns about the inevitability of attack against "critical U.S. infrastructure systems" and

17. Jeh C. Johnson, *Let's Pass Cybersecurity Legislation,* THE HILL (Sept. 9, 2014, 5:30 PM), http://thehill.com/opinion/op-ed/217151-lets-pass-cybersecurity-legislation.

18. *Id.*; Alan W. Ezekiel, *Hackers, Spies, and Stolen Secrets: Protecting Law Firms from Data Theft*, 26 HARV. J. L. & TECH. 649 (2013); *see generally* Xiang Li, *Hactivism and the First Amendment: Drawing the Line Between Cyber Protests and Crime*, 27 HARV. J. L. & TECH. 301 (2013) (discussing hacks and cyber attacks).

19. David M. Morens, *et al*, *Pandemic Influenza's 500th Anniversary,* 51 CLINICAL INFECTIOUS DISEASES 1442 (2010).

20. Laurence Barton, CRISIS LEADERSHIP NOW: A REAL-WORLD GUIDE TO PREPARING FOR THREATS, DISASTER, SABOTAGE, AND SCANDAL 109 (2008).

21. *Id.*

22. Anna Mulrine, *CIA Chief Leon Panetta: The Next Pearl Harbor Could Be a Cyberattack*, CHRISTIAN SCI. MONITOR (June 9, 2011), http://www.csmonitor.com/USA/Military/2011/0609/CIA-chief-Leon-Panetta-The-next-Pearl-Harbor-could-be-a-cyberattack.

says, "[i]t's only a matter of the 'when,' not the 'if,' that we are going to see something dramatic."[23] Other recent examples of cyberattack include the widely discussed breaches at Target,[24] J.P. Morgan Chase,[25] the U.S. Postal Service,[26] Home Depot,[27] the November 2014 breach of Sony Pictures Entertainment,[28] and continued reports of on-going financial institution breaches.[29]

III. TECHNOLOGICAL ISSUES TOO COMPLEX?

Cybersecurity is complicated by the modern environment in which data resides. The rapid rate of technological change results in wonderful new contributions to our daily lives. These technological advances such as cloud computing, smart phones, social media—and, in particular, the Internet of Things (IoT)—brings massive connectivity to our lives in ways not imagined a mere decade or two ago.[30] However, cyber security technologist Bruce

23. Siobhan Gorman, *NSA Chief Warns of 'Dramatic' Cyberattack,* WALL ST. J., Nov. 21, 2014, at A2.

24. *See generally* Lawrence J. Trautman, *Managing Cyberthreat*, 31 SANTA CLARA COMPUTER & HIGH TECH. L.J. (forthcoming 2015), http://ssrn.com/abstract=2534119 (discussing breach of cyber security at Target).

25. Emily Glazer, Danny Yadron & Daniel Huang, *Hackers May Have Targeted at Least 13 Firms*, WALL ST. J., Oct. 9, 2014, at C1; Press Release, Sarah Bloom Raskin, Deputy Sec.'y of the Treasury of the U.S., Remarks Before the Meeting of the Texas Bankers' Association Executive Leadership Cybersecurity Conference: Cybersecurity for Banks: 10 Questions for Executives and Their Boards (Dec. 3, 2014), http://www.treasury.gov/press-center/press-releases/Pages/jl9711.aspx.

26. Laura Stevens & Danny Yadron, *Postal Service Hit by a Vast Data Breach,* WALL ST. J., Nov. 11, 2014, at A4; *Significant Cyber Incidents Since 2006*, CTR. FOR STRATEGIC & INT'L. STUD., http://csis.org/files/publication/141211_Significant_Cyber_Incidents_Since_2006.pdf (last visited Aug. 25, 2015) [hereinafter *Incidents*].

27. *See* Shelly Banjo, *Home Depot Hackers Stole Buyer Email Addresses*, WALL ST. J., Nov. 7, 2014, at A1 (describing Home Depot data breach); *see also* Michael Calia, *Breach Plagues Home Depot,* WALL ST. J., Nov. 19, 2014, at B3 (reporting estimated cost of hacking to be $34 million during 2014).

28. Incidents, *supra* note 26, at 172 (last visited Sept. 22, 2015) (reporting that "Sony Pictures Entertainment is hacked, with the malware deleting data and the hackers posting online employees' personal information and unreleased films. The incident is similar to earlier hacks against South Korean media outlets."). *See* Adrienne Debigare, Rebekah H. Jones & Jiou Park, *2014 Year in Review*, in Urs Gasser, Jonathan Zittrain, Robert Faris & Rebekah H. Jones, *Internet Monitor 2014: Reflections on the Digital World: Platforms, Policy, Privacy, and Public Discourse*, 2014–17 BERKMAN CTR. FOR INTERNET & SOC'Y AT HARV. UNIV. 12, 22 (2014) (discussing the hack of Sony Pictures).

29. *See* David E. Sanger & Nicole Perlroth, *Bank Hackers Steal Millions Via Malware,* N.Y. TIMES, Feb. 14, 2015, at A1 (detailing cyberattacks on more than 100 banks and other financial institutions in thirty nations).

30. The following discuss examples of new forms of connectivity. *E.g.*, Adam D. Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation*, 21 RICH. J.L. & TECH. 6 (2015); Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security & Consent*, TEX. L. REV. (2014), http://ssrn.com/abstract=2409074; Lee W. McKnight, *Over the Virtual Top. Digital Service Value Chain Disintermediation Implications for Hybrid Heterogeneous Network Regulation*, 42ND TPRC RESEARCH CONF. ON INFO., COMM., AND INTERNET POL'Y, GEO. MASON U. SCH. OF LAW (Sept. 12–14, 2014), http://ssrn.com/abstract=2495901; Matthew B. Becker, *Interoperability Case Study: Electronic Data Interchange (EDI)*, 2012–15 BERKMAN CTR. FOR INTERNET & SOC'Y AT HARV. UNIV. (Mar. 2012), http://ssrn.com/abstract=2031109; Tijmen Wisman, *Purpose and Function Creep by Design: Transforming the Face of Surveillance through the Internet of Things*, 4 EURO. J. L. & TECH. (2013), http://ssrn.com/abstract=2486441; Christina Mulligan, Personal Property Servitudes on the Internet of Things (July 14, 2014), Brook. L. Sch., Legal Studies Paper No. 400, http://ssrn.com/abstract=2465651; Edith Ramirez, Chairwoman, U.S. Fed. Trade Comm'n: Opening Remarks Before Int'l Consumer Electronics Show: Privacy and the IoT: Navigating Privacy Issues (Jan. 6, 2015), http://www.ftc.gov/system/files/documents/

Schneier believes we are (1) progressively losing control of the IT infrastructure; (2) attacks are getting much more sophisticated; and (3) we are seeing increased government involvement worldwide.[31] Schneier's thesis is that with the rise of cloud computing, organizations are progressively outsourcing much or even most of their infrastructure.[32] As a result, the security of this data can no longer be controlled.[33] Increased technological advances result in capabilities that increasingly present as war-like tactics.[34]

Serving as the SEC's inaugural Director of the Division of Risk, Strategy, and Financial Innovation (2009–2011), Professor Henry T.C. Hu concludes that "modern financial innovation has resulted in objective realities that are far more complex than in the past, often beyond the capacity of the English language, accounting terminology, visual display, risk measurement, and other tools on which all depictions must primarily rely."[35] These same characteristics of highly sophisticated data encryption and transmission systems apply communications systems as well. Professor Hu further observes that "such characteristics can be so complex that even 'objective reality' is subject to multiple meanings."[36]

In cyberspace, as Lawrence Lessig says, "[c]ode is law."[37] James Grimmelman observes that "[u]nlike the rule of law, the rule of software is simple and brutal; whoever controls the software makes the rules. And, if power corrupts, then automatic power corrupts automatically."[38] Complex technology affords many entry points for attackers to find vulnerabilities, and "cybersecurity is in many ways an arms race between attackers and defenders."[39] A recent report by the Congressional Research Service warns that "[d]efenders can often protect against weaknesses, but three are particularly challenging: inadvertent or intentional acts by *insiders* with access to a system; *supply chain* vulnerabilities, which can permit the insertion of malicious software or hardware during the acquisition process; and previously unknown, or *zero-day*, vulnerabilities with no established fix."[40]

A. Pervasive Knowledge Gap

Much like the technological mechanisms of the Ebola virus, technical

---

public_statements/617191/150106cesspeech.pdf; PETER H. DIAMANDIS & STEVEN KOTLER, BOLD: HOW TO GO BIG, CREATE WEALTH, AND IMPACT THE WORLD (Simon & Schuster, 2015).

31. *See* Bruce Schneier, InfoQ, Keynote Address at QCon (Dec. 12, 2014), http://www.infoq.com/presentations/Schneier-security-keynote-qcon (describing the role of cloud computing).

32. *Id.*

33. *Id.*

34. *Id.*

35. Henry T.C. Hu, *Too Complex to Depict? Innovation, "Pure Information," and the SEC Disclosure Paradigm*, 90 TEX. L. REV. 1601, 1602 (June 2012) (describing the environment of risk inherent in complex financial instruments associated with and subsequent to the 2008–2009 global financial crisis).

36. *Id.*

37. Bitcoin, *supra* note 15.

38. *Id.*

39. Eric A. Fischer, CONG. RES. SERV., R43831, IN FOCUS: CYBERSECURITY ISSUES AND CHALLENGE, 1 (Dec. 16, 2014).

40. *Id.*

issues surrounding cybersecurity are not widely understood by the general public. Former CIA Director General Michael Hayden describes a dangerous digital and cybersecurity knowledge gap that exists because "[t]oday's youth are 'digital natives,' having grown up in a world where computers have always existed and seem a natural feature. But the world is still mostly led by 'digital immigrants,' older generations for whom computers and all the issues the Internet age presents remain unnatural and often confusing."[41] Many of our business and governmental leaders are now over the age of fifty. As a result, few in this demographic used a personal computer during their college education years. Therefore, computer usage and experience for most of this leadership group has been only during recent years and often for many fewer hours than for someone twenty years younger. To better place this important issue in perspective, Singer and Friedman observe that,

> As late as 2001, the Director of the FBI did not have a computer in his office, while the US Secretary of Defense would have his assistant print out e-mails to him, write his response in pen, and then have the assistant type them back in. This sounds outlandish, except that a full decade later the Secretary of Homeland Security, in charge of protecting the nation from cyberthreats, told us at a 2012 conference, "Don't laugh, but I just don't use e-mail at all." It wasn't a fear of security, but that she just didn't believe e-mail useful. And, in 2013, Justice Elena Kagan revealed the same was true of eight out of nine of the United States Supreme Court justices, the very people who would ultimately decide what was legal or not in this space.[42]

Other lawmakers who admit to not using email include Senators John McCain and Lindsey Graham.[43] And they are not alone according to *Meet the Press* host Chuck Todd who observes, "a bunch of senators looked up from their typewriters to say they don't use email either. So our luddite caucus includes Tom Carper from Delaware, Orrin Hatch, Pat Roberts, Chuck Schumer said if he started emailing, he'd never stop, and Richard Shelby of Alabama."[44] Technological advances are coming at such an accelerated rate that it is not surprising that voters and legislators do not appear "engaged on any cybersecurity concerns."[45] Singer and Friedman believe that issues surrounding cybersecurity are "perceived as too complex to matter in the end to voters, and as a result, the elected representatives who will decide the issues on their behalf. This is one of the reasons that despite all these bills no substantive cybersecurity legislation was passed" until December 2014, more than a decade following presidential signature on a 2002 bill.[46]

---

41. P.W. SINGER & ALLAN FRIEDMAN, CYBERSECURITY AND CYBERWAR: WHAT EVERYONE NEEDS TO KNOW 4 (Oxford University Press 2014) [hereinafter *Singer & Friedman*].

42. *Id.*

43. *Meet the Press Transcript* (Mar. 15, 2015), http://www.nbcnews.com/meet-the-press/meet-press-transcript-march-15-2015-n323871.

44. *Id.*

45. Singer & Friedman, *supra* note 41, at 8.

46. *Id.*

IV. CYBERSECURITY CONSTITUENCIES

For purposes of policy analysis, let us consider the following cybersecurity constituency groups within the United States: (1) *Consumers*; (2) *Investors*; (3) *Law enforcement*; (4) *Business;* (5) *Federal, State and Local Government;* and (6) *National Security* interests. Note that individuals will play various roles from time-to-time (as consumers, investors, or perhaps as small business owners). And, our *Federal, State and Local Government* and *National Security* institutions exist as agents of U.S. citizens. In the United States, "[w]hile a high proportion of internet infrastructure is private, and government has carved out a central role in cybersecurity, action taken by government and corporate actors has been highly fragmented."[47]

As expected, tensions exist between these various groups as each seeks to maximize its own perceived interest or mission. Economists might suggest that *Consumers*, *Investors*, and *Business* interests will each seek to maximize their position by increasing income and avoiding costs. Because cybersecurity involves highly complex technological issues (and usually hidden costs), many constituencies will find it difficult to obtain or perceive accurately the information necessary to determine their own best interest. Jonathan Zittrain observes, "[f]urther complicating matters, trust in government to address concerns around cybersecurity is at a low point, and the level of engagement by civil society groups and academia has been lacking."[48]

Much like the recent Ebola outbreak, many seem to agree that cybersecurity is a major threat, capable of bringing both economic and other aspects of daily life to a halt.[49] First, a brief look at cyber threat issues facing each of these constituency groups.

A. Consumers

Consumers today experience "little of their existence that is not either directly mediated through digital means or recorded by digital devices; sleep cycles; work history; health information; financial records; social networks; shopping culture; tastes in music, literature, and movies; some heating schedules; and preferences in romantic partners."[50] Consumers fall victim on a daily basis to various "*carding* crimes—offenses in which the Internet is used to traffic in and exploit the stolen credit card, bank account, and other personal identification information of hundreds of thousands of victims globally."[51] In just one instance, FBI allegations "chronicle a breathtaking spectrum of cyber

47. Zittrain, *supra* note 5.

48. *Id.*

49. Gorman, *supra* note 23.

50. Robert Faris & Rebekah Heacock Jones, *Platforms and Policy*, in INTERNET MONITOR 2014: REFLECTIONS ON THE DIGITAL WORLD: PLATFORMS, POLICY, PRIVACY, AND PUBLIC DISCOURSE, 28, 28 (Berkman Ctr. Res. Publ'n No. 2014–17, Dec. 15, 2014).

51. Press Release, FBI, Manhattan U.S. Attorney and FBI Assistant Dir. in Charge Announce 24 Arrests in Eight Countries as Part of Int'l Cyber Crime Takedown (June 26, 2012), http://www.fbi.gov/newyork/press-releases/2012/manhattan-u.s.-attorney-and-fbi-assistant-director-in-charge-announce-24-arrests-in-eight-countries-as-part-of-international-cyber-crime-takedown.

schemes and scams . . . individuals sold credit cards by the thousands and took the private information of untold numbers of people . . . offer[ing] every stripe of malware and virus to fellow fraudsters."[52] According to the FBI, "*[c]arding* refers to various criminal activities associated with stealing personal . . . and financial information . . . including the account information associated with credit cards, bank cards, debit cards, or other access devices—and using that information to obtain money, goods, or services without the victims' authorization or consent . . . ."[53] In addition, "*carding forums* . . . exchange information related to carding . . . hacking methods or computer-security vulnerabilities that could be used to obtain personal identification information; and to buy and sell . . . stolen . . . account numbers, hardware for creating counterfeit . . . cards, or goods bought with compromised . . . card accounts."[54] University of Buffalo mathematics Professor Thomas Cusick contrasts the U.S. experience to that of Europe.[55] Professor Cusick notes that unlike in Europe where a more sophisticated chip card has been in use for the past decade:

> [U]ntil very recently credit card issuers in the United States have only used the magnetic strip cards, which have much weaker security features than chip cards . . . [U.S.] issuers have not wanted to roll out chip cards, because there were very few merchants who had the terminals to accept them. Merchants have not wanted to incur the significant cost to buy the new chip terminals, because so few Americans had chip cards.[56]

Consumer behavioral change is now possible because of major breaches such as at Target; but "[e]ven with these incentives, the American banks have only rolled out 'chip and signature' cards, which are less expensive than the much more secure 'chip and pin' cards which are ubiquitous in Europe."[57] With each day that passes, consumers purchase automobiles, household devices, and life-dependent medical products and devices that connect to the Internet. Given that the total number of Internet of Things (IoT) developers are projected to increase from 0.8 million in 2015 to 4.5 million during 2020,[58] it is reasonable to assume that many products will be designed and manufactured by parties having little or no prior experience in bringing cyber secure products to market.

Almost without exception, consumers by the millions lack the resources and knowledge of all things cyber to mount any kind of effective defense

---

52. *Id.*

53. *Id.*

54. *Id.*

55. Email from Thomas Cusick, Professor of Mathematics, Univ. at Buffalo to Lawrence J. Trautman (Mar. 18, 2015, 12:47 CST) (on file with author).

56. *Id.*

57. *Id.*

58. *See The Connected World: Examining the Internet of Things: Hearing Before the S. Comm. on Com., Sci., and Transp.*, 114th Cong. (2015), (testimony of Adam D. Thierer, Senior Research Fellow, Mercatus Center at Geo. Mason U.) (citing STIJN SCHUERMANS & MICHAEL VAKULENKO, IOT: BREAKING FREE FROM INTERNET AND THINGS 7 (VisionMobile 2014) (showing via chart anticipated expansion of IoT technology)); *see also* Warren Kurisu, *Securing IoT Devices with ARM TrustZone*, EE TIMES (Aug. 15, 2014) (discussing the need for security in IoT systems), http://www.eetimes.com/author.asp?doc_id=1323543.

against an attack to any of their personal data devices. Issues of online security are inextricably linked to considerations of consumer privacy and governmental surveillance.[59] Robert Faris and David R. O'Brien state that "the same architectures that allow private companies to collect personal data or encourage us to share this data also offer openings for third parties to access this same data, some of which is voluntary, [data sale to advertisers] . . . some compulsory (e.g. government data requests), and some involuntary (e.g. cyberattacks)."[60] Consumers are vulnerable to breaches of their personal data wherever it resides (stores, hospitals, department of motor vehicles, educational institutions, etc.). Faris and O'Brien observe:

> [U]sers are not in a position to fully and accurately evaluate how well companies protect their privacy and security. Bruce Schneier describes this asymmetric user-company relationship as "digital feudalism," in the sense that the privacy and security of users is tied to the decisions of their providers, over which they have no power and little knowledge.[61]

Understandably, consumers are profoundly apprehensive upon learning of a major breach, due to the amount of time required to contact creditors and attempt to resolve a financial nightmare experienced by all too many. President Obama observes, "[a]s consumers, we do more online than ever before. We manage our bank accounts. We shop. We pay our bills. We handle our medical records . . . . But it also means that this problem of how we secure this digital world is only going to increase."[62]

Much like the threat of Ebola infection, on an individual level the American public is essentially helpless to mount an effective defense against such a menace as cyberthreat. Just as in the case of national security matters and issues involving war, it appears consumers need to rely on their government to protect them.

B. Investors

Mandatory disclosure of material corporate information to investors is a "defining characteristic of U.S. securities regulation."[63] Regarding disclosure of cyber risks, the SEC recognizes the tension between required disclosure to investors and the potential harm to companies by providing too much detailed information to criminals. Accordingly, the Division guidance states, "[w]e are

59. Robert Faris & David R. O'Brien, *Data and Policy*, *in* INTERNET MONITOR 2014: REFLECTIONS ON THE DIGITAL WORLD: PLATFORMS, POLICY, PRIVACY, AND PUBLIC DISCOURSE 63, 63 (Berkman Ctr. Res. Publ'n No. 2014–17, Dec. 15, 2014).

60. *Id.*

61. *Id.* at 64 (citing Bruce Schneier, *Power in the Age of the Feudal Internet*, *in* INTERNET MONITOR 2013: REFLECTIONS ON THE DIGITAL WORLD 10, 10 (Berkman Ctr. Res. Publ'n No. 2013–27, Dec. 12, 2013)).

62. President Barack Obama, Remarks by the President at the Cybersecurity and Consumer Protection Summit (Feb. 13, 2015), http://www.whitehouse.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit.

63. *See* Stephen M. Bainbridge, *Mandatory Disclosure: A Behavioral Analysis*, 68 U. CIN. L. REV. 1023, 1023 (2000) (citing Europe & Overseas Commodity Traders v. Banque Paribas London, 147 F.3d 118, 126 (2d Cir. 1998) ("Through mandatory disclosure, Congress sought to promote informed investing and to deter the kind of fraudulent salesmanship that was believed to have led to the market collapse of 1929.")).

mindful of potential concerns that detailed disclosures could compromise cybersecurity efforts—for example, by providing a 'roadmap' for those who seek to infiltrate a registrant's network security—and we emphasize that disclosures of that nature are not required under the federal securities laws."[64] Examples of "[c]yber attacks include . . . gaining unauthorized access to digital systems for purposes of misappropriating assets or sensitive information, corrupting data, or causing operational disruption. Cyber attacks may also be carried out in a manner that does not require gaining unauthorized access, such as by causing denial-of-service attacks on websites."[65] Successful cyber attacks may result in substantial costs to companies victimized and other negative consequences may include: "remediation costs; increased cybersecurity protection costs; lost revenues; litigation; and reputational damage."[66]

The SEC provides numerous alerts designed to advise investors about common cyber threats,[67] and examines broker-dealer and investment advisers for compliance with cybersecurity directives.[68] In an effort to provide investors with material information to enable informed investment decisions, the SEC requires disclosure by registrants of the "risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky . . . we expect registrants to evaluate their cybersecurity risks and take into account all available relevant information, including prior cyber incidents and the severity and frequency of those incidents."[69] The SEC believes disclosure considerations should include the probability of incident and "the quantitative and qualitative magnitude of those risks, including the potential costs and other consequences resulting from misappropriation of assets or sensitive information, corruption of data or operational disruption."[70]

Here, we find another example where public policy may be at cross-purposes. In an attempt to protect the investing public, the SEC requires disclosure of perceived risk to cyberattack and disclosure of material data breaches.[71] In some breach cases, it is possible that the SEC disclosure requirements may be in conflict with attempts to monitor and map the sources

64. SEC DIV. OF CORP. FIN., *infra* note 89.

65. *Id.*

66. *Id.*

67. Press Release, SEC Alerts Investors, Industry on Cybersecurity (Feb. 3, 2015), http://www.sec.gov/news/pressrelease/2015-20.html#.VOaUJfnF-Hg; Investor Bulletin: Protecting Your Online Brokerage Accounts from Fraud, U.S. SEC. AND EXCH. COMM'N (Feb. 3, 2015), http://www.sec.gov/oiea/investor-alerts-bulletins/ib_protectaccount.html#.VOapLvnF-Hg.

68. *Cybersecurity Examination Sweep Summary*, NAT'L EXAM PROGRAM RISK ALERT (Office of Compliance Inspections and Examinations) Feb. 3, 2015, http://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf.

69. SEC DIV. OF CORP. FIN., *infra* note 89, at 2–3.

70. *Id.* at 3.

71. Luis A. Aguilar, Commissioner, U.S. Securities and Exchange Commission, Remarks at SEC Speaks: Addressing Known Risks to Better Protect Investors (Feb. 21, 2014), http://www.sec.gov/News/Speech/Detail/Speech/1370540828740#.VK_SKCvF-Hg; Luis A. Aguilar, Commissioner, U.S. Securities and Exchange Commission, Statement at the Commission's Role in Addressing the Growing Cyber-Threat (Mar. 26, 2014) http://www.sec.gov/News/PublicStmt/Detail/ PublicStmt/1370541287184#.VK_RQyvF-Hg.

and methods employed by a cyber attacker.

C. Law Enforcement

Just like in the case of the Ebola threat, state and local law enforcement needs to look to the federal government for help. The *2014 Quadrennial Homeland Security Review* ("2014 Review"), described more fully later, provides a description of the strategic environment, guiding principles, strategic priorities (such as securing against the evolving threat of terrorism), biological hazards and threats, potential nuclear terrorism, impact of immigration challenges, and associated issues.[72]

Cyberspace has brought technological advantage to traditional crimes, including "the production and distribution of child pornography and child exploitation conspiracies, banking and financial fraud, intellectual property violations, and other crimes, all of which have substantial human and economic consequences."[73] FBI Assistant Director Richard McFeely observes, "[s]ince 2008, our economic espionage arrests have doubled; indictments have increased five-fold; and convictions have risen eight-fold."[74]

D. Business

By now, everyone engaged in business should know that cyber security is an important strategic and governance issue.[75] Andrew H. Tannenbaum, Cybersecurity Counsel at IBM, observes, "[v]aluable intellectual property that took companies years to develop has been stolen in milliseconds."[76] Senator Joseph Lieberman states, "[e]xtremely valuable intellectual property is being stolen regularly by cyber exploitation, by people and individuals and groups and countries abroad . . . this means jobs are being created abroad that would otherwise be created here."[77] SEC Commissioner Aguilar warns, "cyber-

72. U.S. DEP'T HOMELAND SEC., 2014 QUADRENNIAL HOMELAND SEC. REV. 26 (2014); *see generally* Trautman, *Virtual Currencies supra* note 15 (describing how virtual currencies have gained traction); Lawrence J. Trautman & Alvin Harrell, *Bitcoin vs. Regulated Payment Systems: What Gives?*, 69 CONSUMER FIN. L.Q. REP. (forthcoming 2015); Lawrence J. Trautman & George P. Michaely, *The SEC & the Internet: Regulating the Web of Deceit*, 68 CONSUMER FIN. L.Q. REP. (forthcoming 2015) (discussing new challenges faced by the SEC with the expanded role of the internet in American society).

73. U.S. DEP'T HOMELAND SEC., *supra* note 72, at 39.

74. Press Release, U.S. Dep't of Justice, Sinovel Corporation and Three Individuals Charged in Wisconsin with Theft of Amsc Trade Secrets (June 27, 2013), http://www.justice.gov/opa/pr/2013/June/13-crm-730.html. *See also* Fernando M. Pinguelo & Bradford W. Muller, *Virtual Crimes, Real Damages: A Primer on Cybercrimes in the United States and Efforts to Combat Cybercriminals*, 16 VA. J.L. & TECH. 116, 126 (2011) (detailing the threat of malicious insiders); Joshua Nathan Aston, *Narco-Terrorism—A Critical Study* (Jan. 29, 2013) (explaining the narcotics nexus with globalization).

75. *See generally* Lawrence J. Trautman & Kara Altenbaumer-Price, *The Board's Responsibility for Info. Tech. Governance*, 28 J. MARSHALL J. COMPUTER & INFO. L. 313 (2011) (sounding an alarm about the escalating cyber security threats facing management of every enterprise).

76. *The Growing Cyber Threat and its Impact on Am. Bus.*: *Hearings Before the H. Permanent Select Comm. on Intelligence*, 114th Cong. 1 (2015) (statement of Andrew H. Tannenbaum, Cybersecurity Counsel, IBM), http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/TannenbaumSFR03192015.pdf.

77. *See* Lieberman, *supra* note 15, at 1 (describing the weakness in government cyber architecture).

attacks have become increasingly costly to companies that are attacked."[78] Deputy Treasury Secretary Sarah Bloom Raskin states, "what we can be sure of is that the financial costs are real and increasing; they stem from the disruption of business, erosion of customers, and the associated loss of revenue, from expenses incurred to secure systems, and appropriately notify customers."[79] While these costs attributable to cybersecurity losses vary dramatically, according to one 2013 survey the "average annualized cost of cyber-crime to a sample of U.S. companies was $11.6 million per year, representing a 78% increase since 2009."[80] The Financial Services Round Table reports, "[f]inancial institutions dedicate significant resources on cybersecurity to stay ahead of the threats. However, the overall 'internet economy' continues to lose an estimated fifteen to twenty percent of the nearly $2–3 trillion it generates annually to cybercrime . . . ."[81] Credit card and electronic payments giant Total System Services, Inc. (TSYS) employs over 10,000 and serves "nearly 400 card-issuing clients in eighty-five countries and more than two million merchants in all fifty states."[82] John Latimer, TSYS Chief Risk and Compliance Officer contends:

> [W]e believe protecting the payments space must be viewed as a national security priority and as such, all of us . . . industry, law enforcement, intelligence agencies, DHS and even DoD . . . must work together to counter the threats of criminals, rogue nation states, hacktivists, and terrorists. We can no longer allow ourselves to be segmented because of security clearances and turf battles and we would solicit [the House Permanent Select Committee on Intelligence] to help remove these barriers to information sharing. This is especially important as the threat of terrorist activity against the financial services sector continues to increase.[83]

Other hard-to-quantify non-financial costs include such items as: "reputational damage and loss of confidence . . . and the loss of sensitive or confidential personal and business information."[84] In testimony before the U.S. House of Representatives Permanent Select Committee on Intelligence, Richard Bejtlich reports:

> We have discovered and countered nation-state actors from China, Russia, Iran, North Korea, Syria, and other countries. The Chinese and Russians tend to hack for commercial and geopolitical gain.

78. *See* Aguilar, *supra* note 14, at 2 (detailing the risks to corporate governance from cyberspace).

79. Raskin, *supra* note 25.

80. *See* Aguilar, *supra* note 14, at 2 (citing Press Release, U.S. Sec. and Exch. Comm'n, HP Reveals Cost of Cybercrime Escalates 70 Percent, Time to Resolve Attacks More Than Doubles (Oct. 8, 2013), http://www8.hp.com/us/en/hp-news/press-release.html).

81. Press Release, Fin. Services Roundtable, FSR Commends Senate Intel Committee's Forward Momentum on Information Sharing Bill (Mar. 17, 2015), http://fsroundtable.org/fsr-commends-senate-intel-committees-forward-momentum-on-information-sharing-bill/.

82. *The Growing Cyber Threat and its Impact on American Business*: *Hearings Before the H. Permanent Select Comm. on Intelligence*, 114th Cong. 1 (2015) (discussing testimony of John Latimer, Chief Risk and Compliance Officer, Total System Services, Inc.), http://docs.house.gov/meetings/IG/IG00/20150319/103149/ HHRG-114-IG00-20150319-SD003.pdf.

83. *Id.* at 8.

84. *See* Raskin, *supra* note 25 (exploring cyberattacks on multinational corporations).

> The Iranians and North Koreans extend these activities to include disruption via denial of service and sabotage using destructive malware. Activity from Syria relates to the regional civil war and sometimes affects Western news outlets and other victims. Eastern Europe continues to be a source of criminal operations, and we worry that the conflict between Ukraine and Russia will extend into the digital realm . . . . The median amount of time from an intruder's initial compromise, to the time when a victim learns of a breach, is currently 205 days . . . nearly 7 months after gaining initial entry.[85]

Expensive cyber regulation impacting business comes from many sources—yet breaches escalate. Effective February 28, 2010, SEC rules amended Item 407 of Regulation S-K to require disclosure about the board's role in a company's risk oversight process, its leadership structure, and "to describe how the board administers its risk oversight function, such as through the whole board, or through a separate risk committee or the audit committee, for example."[86] The Dodd-Frank Act requires large financial institutions to establish independent risk committees on their boards,[87] with at least one member of the committee required to have risk management experience at a large, complex firm.[88] As the result of the proliferation of cyberattacks during 2010 and 2011, the SEC's Division of Corporation Finance announced on October 13, 2011 disclosure guidance for cybersecurity issues.[89] The Division of Corporation Finance states, "[f]or a number of years, registrants have migrated toward increasing dependence on digital technologies to conduct their operations. As this dependence has increased, the risks to registrants associated with cybersecurity have also increased, resulting in more frequent and severe cyber incidents."[90] Litigation arising from potential cybersecurity liability exposure may cause businesses to sustain significant expense."[91] President Obama observes:

> As a nation, we do more business online than ever before—trillions of dollars a year. And high-tech industries, like those across the [Silicon] Valley, support millions of American jobs. All this gives us an enormous competitive advantage in the global economy. And

85. *Understanding the Cyber Threat and Implications for the 21st Century Econ.*: *Hearings Before the Subcomm. on Oversight and Investigations*, 114th Cong. 1 (2015) (statement of Richard Bejtlich, Chief Security Strategist, FireEye, Inc.), http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/BejtlichSFR03192015.pdf. (citing Thomas Rid & Ben Buchanan, *Attributing Cyber Attacks*, 39 J. STRATEGIC STUDIES 4 (2014), http://www.tandfonline.com/doi/abs/10.1080/01402390.2014.977382).

86. Proxy Disclosure Enhancements Rule, SEC Release No. 33-9089, 34-61175 (Dec. 16, 2010).

87. JOHN LESTER & JOHN BOVENZI, THE DODD-FRANK ACT: WHAT IT DOES, WHAT IT MEANS, AND WHAT HAPPENS NEXT, 3 (2010).

88. *Id.*; *see also* SCOTT E. LANDAU, KATHLEEN D. BARDUNIAS & KIMBERLY E. MORITZ, DODD-FRANK ACT REFORMS EXEC. COMPENSATION AND CORPORATE GOVERNANCE FOR ALL PUBLIC COMPANIES (July 15, 2010), http://www.pillsburylaw.com/publications/dodd-frank-act-reforms-executive-compensation-and-corporate-governance-for-all-public-companies (explaining risk management is required for large firms).

89. SEC DIV. OF CORP. FIN., CF DISCLOSURE GUIDANCE: TOPIC NO. 2 CYBERSECURITY (Oct. 13, 2011), http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

90. *Id.*

91. Kevin M. Gatzlaff & Kathleen A. McCullough, *The Effect of Data Breaches on Shareholder Wealth*, 13 RISK MGMT. & INS. REV. 1 (2010).

> for that very reason, American companies are being targeted, their trade secrets stolen, intellectual property ripped off. The North Korean cyber attack on Sony Pictures destroyed data and disabled thousands of computers, and exposed the personal information of Sony employees. And these attacks are hurting American companies and costing American jobs. So this is also a threat to America's economic security.[92]

It seems unlikely that most U.S. business executives understand the current and future costs for loss of trade secrets and other intellectual property. Representing many of America's largest financial service companies (asset management, banking, insurance and payment companies), Tim Pawlenty, Chief Executive Officer of the Financial Services Roundtable states:

> The private sector is obviously waging a battle against attacks which are clearly launched by organized crime, other nations, or hostile entities supported by other nations. While the financial sector is an example of strong and frequent cyber collaboration and investment, we cannot fight this battle alone. . . Congress needs to act. In addition, these issues will need to be more aggressively and effectively addressed as part of America's larger foreign policy and security initiatives.[93]

Understandably, executives are busy with day-to-day concerns and not accustomed to or skilled at dealing with abstract concepts they don't believe they can do anything about. For all too many businesses, the aggregate cost to mount a defense against cyber attack appears mind-boggling. Here again, an analogy with the recent Ebola problem is helpful. Just like in the fight against Ebola, only a few select hospitals possess enhanced capabilities necessary to effectively fight the virus. In the case of the American business community, a few select enterprises (having substantial resources) are equipped to attempt to provide effective cybersecurity. However, as we have already seen, reported breaches are rampant, even among companies reasonably considered to have capabilities measuring up to the task. Much like with Ebola, in the United States, the only national institutions having the resources and experience to shoulder this burden is the federal national security infrastructure.

E. Federal, State and Local Government

The Office of Management and Budget (OMB) reports that annual U.S. governmental cybersecurity expenditures for FY2013 alone amounts to $10.34 billion.[94] Despite this high level of monetary expenditures, government

92. Remarks by the President at the Cybersecurity and Consumer Protection Summit (Feb. 13, 2015), http://www.whitehouse.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit.

93. *The Growing Cyber Threat and its Impact on Am. Bus.*: *Hearings Before the H. Permanent Select Comm. on Intelligence*, 114th Cong. 1 (2015) (testimony of Tim Pawlenty, Chief Executive Officer, The Financial Services Roundtable), http://docs.house.gov/meetings/IG/IG00/20150319/103149/HHRG-114-IG00-20150319-SD002.pdf.

94. *See* OFF. OF MGMT. & BUDGET, EXEC. OFF. OF THE PRESIDENT, OMB ANNUAL REPORT TO CONG.: FED. INFO. SEC. MGMT. ACT 1, 59 (2014) (exhibiting the annual U.S. governmental cybersecurity

agencies are a prime target of certain groups intent on creating highly-visible cyber disruption. On June 15, 2011, "Lulz Security, a group of hackers who have been responsible for a number of recent online data breaches, took aim at some United States government agencies . . . ."[95] During the same week, Lulz Security claimed responsibility for several other victims, including an F.B.I. website and an internal file from the U.S. Senate website.[96]

The financial meltdown of 2008–09 "caused most states to severely trim their budgets, reducing their ability to devote expenditures to cyberdefense . . . ."[97] As a result, most states "remain an appealing target for cybercriminals, as their networks hold some of their citizens' most vital information, including health and driving records, educational and criminal records, professional licenses, and tax information."[98] In particular, "State university's [sic] are an especially vulnerable target, as shown in May 2009 when officials at the University of California-Berkeley announced that hackers had stolen the Social Security numbers of approximately 97,000 students, alumni, and others over the course of six months."[99] In addition to their frequent status as victims of cyber breach, state legislatures are also responsible for a hodge-podge of rules and regulations regarding mandatory disclosure of data breaches.[100] Compliance with these well-meaning and sometimes conflicting state requirements may be expensive and ineffective.

F. National Security Interests

The increased reliance on cyber warfare and advances in computer technology as a front line of offensive and defensive national security weapons means that "[c]ybersecurity is the newest and most unique national security issue of the twenty-first century."[101] Deputy Secretary of Defense William Lynn says, "[i]f we can minimize the impact of attacks on our operations and attribute them quickly and definitively, we may be able to change the decision calculus of an attacker . . . . [Lynn noted] a 'foreign intelligence service' had

---

expenditures).

95. Nick Bilton, *Hacking Group Says it Brought Down C.I.A. Site*, N.Y. TIMES (June 15, 2011), http://bits.blogs.nytimes.com/2011/06/15/hacking-group-says-it-brought-down-c-i-a-site/?.

96. *Id.*

97. Fernando M. Pinguelo & Bradford W. Muller, *Virtual Crimes, Real Damages: A Primer on Cybercrimes in the United States and Efforts to Combat Cybercriminals*, 16 VA. J.L. & TECH. 116, 120 (2011) (citing DELOITTE & NASCIO, STATE GOV'TS AT RISK: A CALL TO SECURE CITIZEN DATA AND INSPIRE PUBLIC TRUST (2010), http://www.nascio.org/publications/documents/Deloitte-NASCIOCybersecurityStudy2010.pdf).

98. *Id.*

99. *Id.*

100. *See generally* DAVID FAGAN ET AL., COVINGTON & BURLING, NEW STATE PRIVACY LAWS GO INTO EFFECT ON JAN. 1, 2015 (2014), http://www.cov.com/files/Publication/6dc3fb13-fec2-4d65-ba37-008996cc64d7/Presentation/PublicationAttachment/2918071b-09d4-4fb5-906f-10d1fc44abf4/Client_Alert_New_State_Privacy_Laws_Go_Into_Effect_on_Jan%201.pdf (compiling recently passed privacy laws in various states).

101. Stuart S. Malawer, *Cyber Warfare: Law and Policy Proposals for U.S. and Global Governance*, 58 VA. LAWYER 28, 28 (2010), http://ssrn.com/abstract=1437002 (citing Wesley K. Clark & Peter L. Levin, *Securing the Info. Highway: How to Enhance the United States' Elec. Defs,* FOREIGN AFF., Nov./Dec. 2009, at 2).

stolen 24,000 files from a U.S. defense contractor in a March [2011] cyberattack."[102] Worthy of note, "[e]ach year, a volume of intellectual property exceeding the size of the Library of Congress is stolen from U.S. government and private-sector networks, the [mid-2011] Pentagon strategy document says."[103] U.S. Defense Secretary Leon Panetta "noted a July [2012] attack against Saudi Arabia's state oil company, Aramco, in which a virus erased critical files on some 30,000 computers, replacing them with images of burning American flags."[104] President Obama observes,

> So much of our computer networks and critical infrastructure are in the private sector, which means government cannot do this alone. But the fact is that the private sector can't do it alone either, because it's government that often has the latest information on new threats. There's only one way to defend America from these cyber threats, and that is through government and industry working together, sharing appropriate information as true partners . . . .

During May 2014, the U.S. Department of Justice charged five Chinese hackers, identified as "officers in Unit 61398 of the Third Department of the Chinese People's Liberation Army (PLA)" with cyber espionage directed at six American companies, including: Alcoa; Allegheny Technologies Inc.; U.S. Steel; Westinghouse Electric Co.; U.S. subsidiaries of SolarWorld AG; and others.[105] Richard Clarke, former White House national security advisor to three U.S. presidents, has written "[i]f we discovered Chinese explosives laid throughout our national electrical system, we'd consider it an act of war. China's digital bombs pose as grave a threat."[106] Many nation states with advanced cyber capabilities do not have the same separation between military and business interests as in the United States.[107] The November-December 2014 cyberattack on Sony Pictures Entertainment is attributed to nation-state action by North Korea,[108] resulting in sanctions imposed by the United States government.[109]

---

102. Julian E. Barnes & Siobhan Gorman, *Cyberwar Plan Has New Focus on Deterrence*, WALL ST. J., July 15, 2011, at A5.

103. *Id.*

104. Julian E. Barnes & Siobhan Gorman, *U.S. Readies Defense Against Cyberthreats*, WALL ST. J., Oct. 12, 2012, at A5.

105. Press Release, U.S. Dept. of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage: First Time Criminal Charges are Filed Against Known State Actors for Hacking (May 19, 2014) [hereinafter *Chinese Hackers*], http://www.justice.gov/opa/pr/2014/May/14-ag-528.html.

106. Richard Clarke, Opinion, *China's Cyberassault on Am.*, WALL ST. J., June 15, 2011, at A15; Sonia K. McNeil, *Privacy and the Modern Grid*, 25 HARV. J.L. & TECH. 199 (2011).

107. STUART MALAWER ET AL., GEORGE MASON UNIV. SCH. OF PUB. POL'Y, CYBER SEC. EXPORT MARKETS (2014), http://ssrn.com/abstract=2490014.

108. *See generally* David Robb, *Sony Hack: A Timeline*, DEADLINE HOLLYWOOD (Dec. 22, 2014, 1:25 PM), http://deadline.com/2014/12/sony-hack-timeline-any-pascal-the-interview-north-korea-1201325501/ (detailing the timeline of the Sony hack); Andy Greenberg, *FBI Director: Sony's 'Sloppy' North Korean Hackers Revealed Their IP Addresses*, WIRED (Jan. 7, 2015, 1:51 PM), http://www.wired.com/2015/01/fbi-director-says-north-korean-hackers-sometimes-failed-use-proxies-sony-hack/ (noting the FBI's conclusions that North Korea was behind the Sony hack); Lawrence J. Trautman, *The Sony Hack: Implications for World Order* (forthcoming) (crediting the North Korean government as the source of the hack on Sony).

109. Press Release, The White House, Executive Order—Imposing Additional Sanctions with Respect to N. Kor. (Jan. 2, 2015), http://www.whitehouse.gov/the-press-office/2015/01/02/executive-order-imposing-

Former U.S. National Counterterrorism Center (NCTC) Director Matthew Olsen states that "following the disclosure of the stolen NSA documents, terrorists are changing how they communicate to avoid surveillance. They are moving to more secure communications platforms, using encryption . . . ."[110] While it is clear that certain nation states currently pose an effective cybersecurity threat,[111] can well-financed terrorist groups be far behind? A recent Congressional Research Service report observes that "[t]he federal role in cybersecurity involves both securing federal systems and assisting in protecting nonfederal systems. Under current law, all federal agencies have cybersecurity responsibilities relating to their own systems, and many have sector-specific responsibilities for [critical infrastructure]."[112] In the United States, it appears that governmental national security institutions are the only entities with the knowledge, budget and capacity to effectively defend against these threats.

V. RECENT POLICY DEVELOPMENTS

The chronology of major cyber security policy developments include: creation of the Office of Homeland Security;[113] President Bush's *Critical Infrastructure Protection Board* by Executive Order 13231;[114] the Federal Information Security Management Act of 2002 (FISMA);[115] the Comprehensive National Cybersecurity Initiative (CNCI);[116] Commission on Cybersecurity for the 44th Presidency;[117] publication during 2011 of the DHS *Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise*,[118] President Obama's 2013 Executive Order 13636,[119] President Obama's Presidential Policy Directive-21: Critical

additional-sanctions-respect-north-korea; David E. Sanger & Michael S. Schmidt, *More Sanctions on N. Kor. After Sony Case*, N.Y. TIMES (Jan. 2, 2015), http://www.nytimes.com/2015/01/03/us/in-response-to-sony-attack-us-levies-sanctions-on-10-north-koreans.html.

110. Matthew G. Olsen, Director, National Counterterrorism Center, Address at the Brookings Inst. (Sept. 3, 2014), http://www.brookings.edu/~/media/Events/2014/09/03%20national%20counterterrorism%20center%20threat%20assessment%20isil%20al%20qaeda%20iraq%20syria%20beyond/03%20nctc%20director%20speech.pdf (last visited Aug. 25, 2015); *but see* Lee Baker, *The Unintended Consequences of U.S. Export Restrictions on Software and Online Services for American Foreign Policy and Human Rights*, 23 HARV. J.L. & TECH. 537, 564–65 (2010) (advocating for liberalizing regulations to promote the export of encryption technology).

111. *Chinese Hackers*, *supra* note 105.

112. Fischer, *supra* note 39.

113. Exec. Order No. 13,228, *Establishing the Office of Homeland Security and the Homeland Security Council*, 66 Fed. Reg. 51,812 (Oct. 10, 2001).

114. Exec. Order No. 13,231, *Critical Infrastructure Protection in the Information Age*, 86 Fed. Reg. 53,063 (Oct. 18, 2001).

115. Federal Information Security Management Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899 (2002) (codified as amended in scattered sections of 44 U.S.C., 40 U.S.C., and 15 U.S.C.).

116. *The Comprehensive National Cybersecurity Initiative*, THE WHITE HOUSE, http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative (last visited Aug. 25, 2015).

117. CSIS COMM'N ON CYBERSECURITY FOR THE 44TH PRESIDENCY, CTR. FOR STRATEGIC AND INT'L STUDIES, SECURING CYBERSPACE FOR THE 44TH PRESIDENCY (2008), http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

118. *Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise*, U.S. DEP'T OF HOMELAND SEC. (Nov. 2011), http://www.dhs.gov/blueprint-secure-cyber-future.

119. Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013) [hereinafter Exec. Order 13,636],

Infrastructure Security and Resilience,[120] NIST Framework for Improving Critical Infrastructure Cybersecurity,[121] the Quadrennial Homeland Security Review,[122] SANS Institute Critical Security Controls,[123] and selected ongoing National Institute of Standards and Technology (NIST) initiatives.[124]

A. Office of Homeland Security

Executive Order 13228[125] created the Office of Homeland Security and required the protection of "energy production, transmission, and distribution services and critical facilities; other utilities; telecommunications; . . . nuclear material [facilities]; public and privately owned information systems; special events of national significance; transportation, including railways, highways, shipping ports and waterways; airports and civilian aircraft; livestock, agriculture, [and water and food systems] . . . ."[126]

B. Critical Infrastructure Protection Board

President Bush's *Critical Infrastructure Protection Board* was created by Executive Order 13231.[127] A definition of "critical infrastructure" was contained in the USA PATRIOT Act of 2001 (P.L. 107-56),[128] and the Bush administration's strategy for homeland security is articulated in *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.*[129]

C. Federal Information Security Management Act of 2002

The Federal Information Security Management Act of 2002 (FISMA) is

---

https://www.federalregister.gov/articles/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity.

120. *Fact Sheet: Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive (PPD)—21 Critical Infrastructure Security and Resilience*, U.S. DEP'T OF HOMELAND SEC. (Mar. 2013), http://www.dhs.gov/publication/fact-sheet-eo-13636-improving-critical-infrastructure-cybersecurity-and-ppd-21-critical.

121. *Framework for Improving Critical Infrastructure Cybersecurity*, U.S. NAT'L INST. OF STANDARDS AND TECH. 1 (Feb. 12, 2014), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

122. *The 2014 Quadrennial Homeland Security Review*, U.S. DEP'T. OF HOMELAND SEC. 5 (2014), http://www.dhs.gov/quadrennial-homeland-security-review-qhsr.

123. *Critical Security Controls for Effective Cyber Defense*, SANS INSTITUTE, http://www.sans.org/critical-security-controls (last visited Sept. 22, 2015).

124. *Executive Order 13,636: Cybersecurity Framework*, THE NAT'L INST.OF STANDARDS AND TECH., http://www.nist.gov/cyberframework/ (last visited Sept. 22, 2015).

125. Exec. Order No. 13,228, *supra* note 113, at 51,812.

126. John Moteff & Paul Parfomak, *CRS Report for Congress: Critical Infrastructure and Key Assets: Definitions and Identification*, THE LIBR. OF CONG., CONG. RES. SERV. CRS-6 (Oct. 1, 2004) (*citing* Exec. Order No. 13,228, *supra* note 113, at 51, 813–14).

127. *Id.* (*citing* Exec. Order No. 13,231, *supra* note 114).

128. *See id.* at CRS-6 (defining "critical infrastructure").

129. *See generally The National Strategy for Physical Protection of Critical Infrastructure and Key Assets*, U.S. DEP'T OF HOMELAND SEC. (Feb. 2003), http://www.dhs.gov/national-strategy-physical-protection-critical-infrastructure-and-key-assets (laying out the necessity to protect critical areas around the United States).

intended to provide "a comprehensive framework for supporting the effectiveness of information security controls over information resources that support Federal operations and assets."[130] Under FISMA, the Office of Management and Budget is responsible for development and oversight of "policies, principles, standards, and guidelines on information security . . ." that may bring harm to Federal systems or information.[131] To ensure uniformity in this process, FISMA requires the National Institute of Standards and Technology (NIST) to prescribe standards and guidelines pertaining to Federal information systems."[132] Evolving over time, the major performance metrics now include focus on: "Information Security Continuous Monitoring (ISCM); Trusted Internet Connections (TIC); Strong Authentication: HSPD-12; Portable Device Encryption; Domain Name System Security Extensions (DNSSEC) Implementation and Email Validation; Remote Access; Controlled Incident Detection; Security Training; Automated Detection and Blocking of Unauthorized Software; and Email Encryption."[133] During 2010, OMB expanded the operational role of the U.S. Department of Homeland Security for FISMA-related Federal agency cybersecurity and information systems.[134]

D. Comprehensive National Cybersecurity Initiative

President George W. Bush launched the Comprehensive National Cybersecurity Initiative (CNCI) in National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23) in January 2008.[135] CNCI and its associated activities evolved under the Obama presidency "to become key elements of a broader, updated national U.S. cybersecurity strategy."[136] The CNCI cyber initiatives are designed to achieve the following objectives:

- To establish a front line of defense against today's immediate threats by creating or enhancing shared situational awareness of network vulnerabilities, threats, and events within the Federal Government—and ultimately with state, local, and tribal governments and private sector partners—and the ability to act quickly to reduce our current vulnerabilities and prevent intrusions.
- To defend against the full spectrum of threats by enhancing U.S. counterintelligence capabilities and increasing the security of the

130. OFF. OF MGMT. & BUDGET, EXEC. OFF. OF THE PRESIDENT, ANNUAL REPORT TO CONG.: FED. INFO. SEC. MGMT. ACT 1 (May 1, 2014), http://www.ferc.gov/media/headlines/2014/2014-4/11-13-14-fisma-report.pdf.

131. *Id.*

132. *Id.*

133. *Id.* at 11.

134. OFF. OF MGMT. & BUDGET, EXEC. OFF. OF THE PRESIDENT, OMB M-10-28, CLARIFYING CYBERSECURITY RESPONSIBILITIES AND ACTIVITIES OF THE EXEC. OFF. OF THE PRESIDENT AND THE DEP'T OF HOMELAND SEC. (DHS) (July 6, 2010), www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-28.pdf.

135. *The Comprehensive Nat'l Cybersecurity Initiative*, THE WHITE HOUSE, http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative (last visited Sept. 22, 2015).

136. *Id.*

supply chain for key information technologies.

- To strengthen the future cybersecurity environment by expanding cyber education; coordinating and redirecting research and development efforts across the Federal Government; and working to define and develop strategies to deter hostile or malicious activity in cyberspace.

In building the plans for the CNCI, it was quickly realized that these goals could not be achieved without also strengthening certain key strategic foundational capabilities within the government. Therefore, the CNCI includes funding within the federal law enforcement, intelligence, and defense communities to enhance such key functions as criminal investigation; intelligence collection, processing, and analysis; and information assurance critical to enabling national cybersecurity efforts . . . . In accord with President Obama's declared intent to make transparency a touchstone of his presidency, the Cyberspace Policy Review identified enhanced information sharing as a key component of effective cybersecurity. To improve public understanding of Federal efforts, the Cybersecurity Coordinator has directed the release of the following summary description of the CNCI . . . . Details [I have included only topic headings here]:

1. Manage the Federal Enterprise Network as a single network enterprise with trusted internet connections.
2. Deploy an intrusion detection system of sensors across the Federal enterprise.
3. Pursue deployment of intrusion prevention systems across the Federal enterprise.
4. Coordinate and redirect research and development (R&D) efforts.
5. Connect current cyber ops centers to enhance situational awareness.
6. Develop and implement a government-wide cyber counterintelligence (CI) plan.
7. Increase the security of our classified networks.
8. Expand cyber education.
9. Define and develop enduring "leap-ahead" technology, strategies, and programs.
10. Define and develop enduring deterrence strategies and programs.
11. Develop a multi-pronged approach for global supply chain risk management.
12. Define the Federal role for extending cybersecurity into critical infrastructure domains.[137]

137. *Id.* at 1–5.

E. Commission on Cybersecurity for the 44th Presidency

The Commission on Cyber Security for the 44th Presidency was established during 2007 by the Center for Strategic and International Studies (CSIS), a Washington, D.C.-based nonpartisan, nonprofit research center.[138] Members of the Commission bring both extensive government experience and are cybersecurity experts.[139] The nonpartisan Commission's research and policy recommendations seek to achieve comprehensive strategy for cyber security improvement in both U.S. critical infrastructure and federal systems.[140] Considering such factors as "federal organization and strategy, cybersecurity norms and authorities, investment and acquisition policy, and government engagement with the private sector[,]" the Commission outlines

> a forward-looking framework for organizing and prioritizing government efforts to secure cyberspace . . . to assess current and future threats to federal systems and to critical infrastructure; review authorities, policies, and government organization for cybersecurity; and identify requirements for critical infrastructure protection, including the need for new incentives, legislation, or regulation.[141]

The final Commission report, *Securing Cyberspace for the 44th Presidency*, was released during December 2008.[142]

F. Blueprint for a Secure Cyber Future

During November 2011, the U.S. Department of Homeland Security published its *Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise*, "designed to protect the critical systems and assets that are vital to the United States, and, over time, to foster stronger, more resilient information and communication technologies to enable government, business and individuals to be safer online."[143] The *Blueprint* provides for two areas of action, "[p]rotecting our Critical Information Infrastructure Today and Building a Stronger Cyber Ecosystem for Tomorrow."[144] In addition, four goals for protecting the critical information infrastructure are listed: "reduce exposure to cyber risk; ensure priority response and recovery; maintain shared situational awareness; and increase resilience."[145]

---

138. *Securing Cyberspace for the 44th Presidency*, CTR. FOR STRATEGIC AND INT'L STUD. 1 (Dec. 2008), http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

139. *Id.* at 1.

140. *Id.* at 1–3.

141. *Comm'n on Cyber Security for the 44th Presidency*, CTR. FOR STRATEGIC AND INT'L STUD. (Jan. 2008), http://csis.org/files/media/csis/pubs/cyber_commission_factsheet.pdf.

142. CTR. FOR STRATEGIC AND INT'L STUD., SECURING CYBERSPACE FOR THE 44TH PRESIDENCY: A REP. OF THE CSIS COMM'N ON CYBERSECURITY FOR THE 44TH PRESIDENCY (2008).

143. U.S. DEP'T OF HOMELAND SEC., BLUEPRINT FOR A SECURE CYBER FUTURE: THE CYBERSECURITY STRATEGY FOR THE HOMELAND SEC. ENTER., ii (2011).

144. *Id.* at iii.

145. *Id.*

G. Policy Objectives

President Obama's 2013 Executive Order[146] directs "the Secretary of the Treasury, along with the Secretary of Commerce and the Secretary of Homeland Security to each make recommendations on a set of incentives that would promote private sector participation in the voluntary program."[147] The Treasury Report further identifies and discusses the following cybersecurity market failures: Underinvestment in knowledge; barriers to information sharing; coordination failures; network externalities; and adverse selection of insurance risks.[148] Next, the Treasury Report turns to a discussion and evaluation of potential government incentives, including: Enhancing information usage capabilities to support information sharing; leveraging framework adoption to clarify liability risk; government funding to encourage basic cybersecurity research; providing technical assistance; further accelerating the security clearance process; potential tax incentives; and cyber insurance.[149] If needed, these government incentives should be appropriately tailored and scaled to the magnitude of the under-investment in cybersecurity; cost-effective; adjust to changing circumstances and availability of new information; coordinated with other incentives; and "motivate private sector entities to expend their own resources to further protect their critical infrastructure assets."[150]

H. Executive Order 13,636 and Critical Infrastructure

On February 12, 2013, President Obama signed Executive Order 13,636, "Improving Critical Infrastructure Cybersecurity," which directs the Executive Branch to:

1. Develop a technology-neutral voluntary cybersecurity framework;
2. Promote and incentivize the adoption of cybersecurity practices;
3. Increase the volume, timeliness and quality of cyber threat information sharing;
4. Incorporate strong privacy and civil liberties protections into every initiative to secure our critical infrastructure; and
5. Explore the use of existing regulation to promote cyber security.[151]

The 2013 Executive Order defines the term "critical infrastructure" to mean "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public

146. Exec. Order No. 13,636, *supra* note 119.

147. U.S. TREASURY DEP'T, REP. TO THE PRESIDENT ON CYBERSECURITY INCENTIVES PURSUANT TO EXEC. ORDER 13,636, 2 (2013) (citing Exec. Order No. 13,636, *supra* note 119, at 11,742).

148. *Id.* at 5–6.

149. *Id.* at 8–25; *see also* Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks*, 88 TEX. L. REV. 1533 (2010) (explaining the risk that civilian networks face in the context of cyber warfare and possible precautions against attacks).

150. U.S. TREASURY DEP'T, REP. TO THE PRESIDENT ON CYBERSECURITY INCENTIVES PURSUANT TO EXEC. ORDER 13636, 5 (2013).

151. Exec. Order No. 13,636, *supra* note 119.

health or safety, or any combination of those matters."[152]

I. Presidential Policy Directive-21

Presidential Policy Directive-21: Critical Infrastructure Security and Resilience, directs the Executive Branch to develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real time; understand the cascading consequences of infrastructure failures; evaluate and mature the public-private partnership; update the National Infrastructure Protection Plan; and develop comprehensive research and development plan.[153]

J. Framework on Improving Critical Infrastructure Cybersecurity

Executive Order 13,636 mandates "development of a voluntary risk-based Cybersecurity Framework—a set of industry standards and best practices to help organizations manage cybersecurity risks.[154] The resulting Framework, created through collaboration between government and the private sector, uses a common language to address and manage cybersecurity risk."[155] Sensitive to imposing additional regulatory requirements on business, the Framework attempts to focus on business needs in a cost-effective way.[156] As a threshold observation, "[t]he Framework complements, and does not replace, an organization's risk management process and cybersecurity program.[157] An organization can use its current processes and leverage the Framework to identify opportunities to strengthen and communicate its management of cybersecurity risk while aligning with industry practices."[158] Of major importance, "an organization without an existing cybersecurity program can use the Framework as a reference to establish one."[159]

The Framework recognizes that "a clear understanding of the organization's business drivers and security considerations specific to its use of [information technology] and [industrial control systems] is required.[160] Because each organization's risk is unique . . . the tools and methods used to achieve the outcomes described by the Framework will vary."[161]

---

152. *Id.*
153. Exec. Order No. 13,636, *supra* note 120.
154. U.S. NAT'L INST. OF STANDARDS AND TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY, VERSION 1.0, 1 (2014) [hereinafter Cybersecurity Framework].
155. *Id.*; *see also* Scott Shackelford, Andrew A. Proia, Brenton Martell & Amanda Craig, *Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable Nat'l and Int'l Cybersecurity Practices,* 50 TEX. INT'L L.J. 303 (2015) (discussing the necessity of implementing standards of cybersecurity to combat cyberattacks).
156. Cybersecurity Framework, *supra* note 154.
157. *Id.* at 4.
158. *Id.*
159. *Id.*
160. *Id.* at 3.
161. *Id.*

K. Transition to Automated Diagnostics and Monitoring

During November 2013, a transition to automated diagnostics and systems monitoring was announced by OMB.[162] This policy goal is stated as "to provide agencies with a policy framework to: monitor their systems on an ongoing basis; evolve from static reauthorizations, or determinations and acceptance of information security risk, to ongoing authorizations of information systems; and create the technological infrastructure to accomplish continuous diagnostics and mitigation and ongoing authorizations."[163]

L. Quadrennial Homeland Security Review ("2014 Review")

The 2014 Review recognizes that "[t]he terrorist threat is increasingly decentralized and may be harder to detect. Cyber threats are growing and pose ever-greater concern to our critical infrastructure systems as they become increasingly interdependent."[164] Accordingly, the 2014 Review recognizes that "DHS must work with both public and private sector partners to share information, help make sure new infrastructure is designed and built to be more secure and resilient, and continue advocating internationally for openness and security of the internet and harmony across international laws to combat cybercrime."[165] To be secure, federal systems and networks must be approached by DHS "as an integrated whole and by researching, developing, and rapidly deploying cybersecurity solutions and services at the pace that cyber threats evolve."[166] And, the 2014 Review acknowledges that "the Federal Government must continue to develop good working relationships with the private sector, lower barriers to partnership, develop cybersecurity best practices, promote advanced technology that can exchange information at machine speed, and build the cyber workforce of tomorrow."[167]

M. SANS Institute Critical Security Controls

Over the years the National Security Agency (NSA) became increasingly concerned that, in everyday practice, efforts to govern data systems and prevent breaches had all too often become "exercises in reporting on compliance and have actually diverted security program resources from the constantly evolving attacks that must be addressed."[168] Accordingly, during 2008 the NSA started "prioritizing a list of the controls that would have the greatest impact in improving risk posture against real-world threats."[169] This

---

162. OFF. OF MGMT. AND BUDGET, Exec. OFF. OF THE PRESIDENT, OMB M-14-03, ENHANCING THE SEC. OF FED. INFO. AND INFO. SYS. (2013).

163. OFF. OF MGMT. AND BUDGET, ANNUAL REP. TO CONG.: FED. INFO. SEC. MGMT. ACT 1 (2014).

164. U.S. DEPT. OF HOMELAND SEC., 2014 QUADRENNIAL HOMELAND SEC. REV. 5 (2014).

165. *Id.* at 7.

166. *Id.*

167. *Id.* at 8.

168. Critical Sec. Controls, *Critical Sec. Controls for Effective Cyber Defense*, SANS INST., http://www.sans.org/critical-security-controls.

169. *Id.*

list of effective security controls ultimately became known as the Critical Security Controls and was coordinated through the SANS Institute, with the Council on CyberSecurity assuming responsibility during 2013.[170] Because the controls are based on an analysis of the most common cyber attack patterns, SANS notes that the Controls are intended to "prioritize and focus on a smaller number of actionable controls with high-payoff, aiming for a 'must do first' philosophy."[171]

N. Ongoing National Institute of Standards & Technology (NIST) Initiatives

The National Institute of Standards & Technology (NIST) continues to offer cybersecurity announcements, tools, and initiatives on an almost daily basis.[172] Those desiring to acquire and maintain a contemporary understanding of cybersecurity developments will likely find the NIST materials of considerable help. A review of the NIST website revealed the following sample of publication drafts or final publications: *NIST Computer Security Division Released DRAFT NISTIR 7621 Revision 1, Small Business Information Security: The Fundamentals* (December 16, 2014); and *Special Publication 800-53A, Revision 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans,* has been approved as final as of December 12, 2014.[173]

O. Presidential 2015 Cybersecurity and Consumer Protection Summit

At a Cybersecurity and Consumer Protection Summit held on February 13, 2015, at Stanford University, President Obama lists the following basic principles to be considered when confronting cyberthreats:

> First, this has to be a shared mission. So much of our computer networks and critical infrastructure are in the private sector, which means government cannot do this alone. But the fact is that the private sector can't do it alone either, because it's government that often has the latest information on new threats. There's only one way to defend America from these cyber threats, and that is through government and industry working together, sharing appropriate information as true partners.
>
> Second, we have to focus on our unique strengths. Government has many capabilities, but it's not appropriate or even possible for government to secure the computer networks of private businesses. Many of the companies who are here today are cutting-edge, but the private sector doesn't always have the capabilities needed during a cyber attack, the situational awareness, or the ability to warn other companies in real time, or the capacity to coordinate a response

170. *Id.*
171. *Id.*
172. *See generally* Computer Security Division News—2015, NAT'L INST. OF STANDARDS AND TECH., http://csrc.nist.gov/news_events/index.html (archiving older documents) (last visited Aug. 25, 2015).
173. *Id.*

> across companies and sectors. So we're going to have to be smart and efficient and focus on what each sector does best, and then do it together.
>
> Third, we're going to have to constantly evolve. The first computer viruses hit personal computers in the early 1980s, and essentially, we've been in a cyber arms race ever since. We design new defenses, and then hackers and criminals design new ways to penetrate them. Whether its phishing or botnets, spyware or malware, and now ransomware, these attacks are getting more and more sophisticated every day. So we've got to be just as fast and flexible and nimble in constantly evolving our defenses.
>
> And fourth, and most importantly, in all our work we have to make sure we are protecting the privacy and civil liberty of the American people.[174]

P. Presidential 2015 Cybersecurity Executive Order

President Obama used the Stanford Cybersecurity and Consumer Protection Summit to announce the creation of a new Cyber Threat Intelligence Integration Center and to sign a new cybersecurity executive order.[175] The president described the purpose of the executive order as "to promote even more information sharing about cyber threats, both within the private sector and between government and the private sector. And it will encourage more companies and industries to set up organizations—hubs—so you can share information with each other."[176]

VI. CONGRESSIONAL ACTION

A. December 2014 Legislation

Many bills about cybersecurity have been introduced since the 111th Congress; "Several passed the House in both the 112th and 113th Congresses. None passed the Senate until the end of the 113th Congress."[177] During December 2014, just hours before the holiday recess, the U.S. Congress passed several major legislative proposals designed to enhance U.S. cybersecurity: the National Cybersecurity Protection Act of 2014[178]; the Federal Information Security Modernization Act of 2014;[179] the Cybersecurity Workforce

174. Press Release, The White House, Remarks by the President at the Cybersecurity and Consumer Protection Summit (Feb. 13, 2015), http://www.whitehouse.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit.

175. *Id.*

176. *Id;. see also* Press Release, The White House, Executive Order—Promoting Private Sector Cybersecurity Information Sharing (Feb. 13, 2015), http://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.

177. ERIC A. FISCHER, Cong. Res. Serv., R42114, FED. LAWS RELATING TO CYBERSECURITY: OVERVIEW OF MAJOR ISSUES, CURRENT LAWS, AND PROPOSED LEGIS. 10 (Dec. 12, 2014).

178. Nat'l Cybersecurity Protection Act of 2014, Pub. L. No. 113-282 (2014).

179. Fed. Info. Sec. Modernization Act of 2014, Pub. L. No. 113-283 (2014).

Assessment Act;[180] The Homeland Security Workforce Assessment Act;[181] and the Cybersecurity Enhancement Act of 2014.[182] A brief outline of the major provisions of each is presented below.

B. The National Cybersecurity Protection Act of 2014

The National Cybersecurity Protection Act of 2014, signed into law by President Obama on December 18, 2014, provides a much needed amendment to the Homeland Security Act of 2002.[183] This law establishes within the Department of Homeland Security (DHS) a National Cybersecurity and Communications Integration Center (NCIC), responsible for sharing cybersecurity risks, incidents, analysis, and warnings for both federal and non-federal entities, overseeing critical infrastructure protection, cybersecurity, and related DHS programs.[184] Major provisions of the law include directing the NCIC to

> (1) enable real-time, integrated, and operational actions across federal and non-federal entities; (2) facilitate cross-sector coordination to address risks and incidents that may be related or could have consequential impacts across multiple sectors; (3) conduct and share analysis; and (4) provide technical assistance, risk management, and security measure recommendations. Directs the center to ensure: [1] continuous, collaborative, and inclusive coordination across sectors and with sector coordinating councils, information sharing and analysis organizations, and other appropriate non-federal partners; [2] development and use of technology-neutral, real-time mechanisms for sharing information about risks and incidents; and [3] safeguards against unauthorized access.[185]

Other provisions of this newly enacted legislation include granting unreviewable discretion to the Under Secretary about decisions regarding, the granting of assistance, provision of information, or granting access to the Center of governmental or private entities.[186] In addition,

> (Sec. 4) Requires the DHS Secretary to submit to Congress recommendations regarding how to expedite implementation of information-sharing agreements for cybersecurity purposes between the center and non-federal entities.
>
> (Sec. 5) Directs the Secretary to report annually to Congress concerning: (1) the number of non-federal participants, the length of time taken to resolve requests to participate in the center, and the reasons for any denials of such requests; (2) DHS's information

180. Cybersecurity Workforce Assessment Act, Pub. L. No. 113-246 (2014).
181. Border Patrol Agent Pay Reform Act of 2014, Pub. L. No. 113-277 (2014).
182. Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274 (2014).
183. Nat'l Cybersecurity Protection Act of 2014, *supra* note 178.
184. *Id.*
185. *Id.*
186. *Id.*

> sharing with each critical infrastructure sector; and (3) privacy and civil liberties safeguards.
>
> (Sec. 6) Requires a Comptroller General (GAO) report on the effectiveness of the center.
>
> (Sec. 7) Directs the Under Secretary to develop, maintain, and exercise adaptable cyber incident response plans to address cybersecurity risks to critical infrastructure.[187]

The law also requires the Secretary to make available to owners and operators of critical infrastructure, information sharing and analysis organizations, and sector coordinating councils the classified national security information program application process for security clearances.[188] In addition to requiring the OMB "to assess agency implementation of data breach notification policies," The National Cybersecurity Protection Act of 2014

> [d]irects the Office of Management and Budget (OMB) to ensure that data breach notification policies require affected agencies, after discovering an unauthorized acquisition or access, to notify: (1) Congress within 30 days, and (2) affected individuals as expeditiously as practicable. Allows the Attorney General (DOJ), heads of elements of the intelligence community, or the Secretary to delay notice to affected individuals for purposes of law enforcement investigations, national security, or security remediation actions.[189]

C. The Federal Information Security Modernization Act of 2014

The Federal Information Security Modernization Act of 2014, signed into law by President Obama on December 18, 2014, provides amendments to the Federal Information Security Management Act of 2002 (FISMA) to "(1) reestablish the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices, and (2) set forth authority for the Secretary of Homeland Security (DHS) to administer the implementation of such policies and practices for information systems."[190] Among its provisions, the Law:

1. Requires the Secretary to develop and oversee implementation of operational directives requiring agencies to implement the Director's standards and guidelines for safeguarding federal information and systems from a known or reasonably suspected information security threat, vulnerability, or risk. Authorizes the Director to revise or repeal operational directives that are not in accordance with the Director's policies.
2. Requires the Secretary (currently, the Director) to ensure the operation of the federal information security incident center (FISIC).
3. Directs the Secretary to administer procedures to deploy technology,

187. *Id.*
188. *Id.*
189. *Id.*
190. Fed. Info. Sec. Modernization Act of 2014, Pub. L. No. 113-283 (2014).

upon request by an agency, to assist the agency to continuously diagnose and mitigate against cyber threats and vulnerabilities.

4. Requires the Director's annual report to Congress regarding the effectiveness of information security policies to assess agency compliance with OMB data breach notification procedures.
5. Provides for OMB's information security authorities to be delegated to the Director of National Intelligence (DNI) for certain systems operated by an element of the intelligence community.
6. Directs the Secretary to consult with and consider guidance developed by the National Institute of Standards and Technology (NIST) to ensure that operational directives do not conflict with NIST information security standards.
7. Directs agency heads to ensure that: (1) information security management processes are integrated with budgetary planning; (2) senior agency officials, including chief information officers, carry out their information security responsibilities; and (3) all personnel are held accountable for complying with the agency-wide information security program.
8. Provides for the use of automated tools in agencies' information security programs, including for periodic risk assessments, testing of security procedures, and detecting, reporting, and responding to security incidents.
9. Requires agencies to include offices of general counsel as recipients of security incident notices. Requires agencies to notify Congress of major security incidents within seven days after there is a reasonable basis to conclude that a major incident has occurred.
10. Directs agencies to submit an annual report regarding major incidents to OMB, DHS, Congress, and the Comptroller General (GAO). Requires such reports to include: (1) threats and threat actors, vulnerabilities, and impacts; (2) risk assessments of affected systems before, and the status of compliance of the systems at the time of, major incidents; (3) detection, response, and remediation actions; (4) the total number of incidents; and (5) a description of the number of individuals affected by, and the information exposed by, major incidents involving a breach of personally identifiable information.
11. Authorizes GAO to provide technical assistance to agencies and inspectors general, including by testing information security controls and procedures.
12. Requires OMB to ensure the development of guidance for: (1) evaluating the effectiveness of information security programs and practices, and (2) determining what constitutes a major incident.
13. Directs FISIC to provide agencies with intelligence about cyber threats, vulnerabilities, and incidents for risk assessments.
14. Directs OMB, during the two-year period after enactment of this Act, to include in an annual report to Congress an assessment of the adoption by agencies of continuous diagnostics technologies and

other advanced security tools.

15. Requires OMB to ensure that data breach notification policies require agencies, after discovering an unauthorized acquisition or access, to notify: (1) Congress within 30 days, and (2) affected individuals as expeditiously as practicable. Allows the Attorney General, heads of elements of the intelligence community, or the DHS Secretary to delay notice to affected individuals for purposes of law enforcement investigations, national security, or security remediation actions.
16. Requires OMB to amend or revise OMB Circular A-130 to eliminate inefficient and wasteful reporting.
17. Directs the Information Security and Privacy Advisory Board to advise and provide annual reports to DHS.[191]

D. The Cybersecurity Workforce Assessment Act

The Cybersecurity Workforce Assessment Act, signed into law by President Obama on December 18, 2014, requires "the Secretary of Homeland Security to assess the cybersecurity workforce of the Department of Homeland Security and develop a comprehensive workforce strategy."[192] The law specifies that the assessment will include "(A) an assessment of the readiness and capacity of the workforce of the Department to meet its cybersecurity mission; (B) information on where cybersecurity workforce positions are located within the Department; [and] (C) information on which cybersecurity positions are . . . performed by [full-time employees, contractors, other agencies, etc,]."[193] In addition, the law provides that within 120 days following enactment, a report will be submitted by the Secretary to appropriate Congressional committees as to "the feasibility, cost, and benefits of establishing a Cybersecurity Fellowship Program to offer a tuition payment plan for individuals pursuing undergraduate and doctoral degrees who agree to work for the Department for an agreed-upon period of time."[194]

E. The Homeland Security Workforce Assessment Act

Signed into law on December 18, 2014, the Homeland Security Workforce Assessment Act became law as an attachment (a rider) to the Border Patrol Agent Pay Reform Act of 2014.[195] This law, in relevant part, is designed to improve compensation rates, retention, and hiring procedures for cybersecurity positions at DHS.[196] The law provides for an enhanced process to identify critical department IT cybersecurity skills and provides for "rates of pay provided for employees in comparable positions in the Department of Defense and subject to the same limitations on maximum rates of pay

191. *Id.*
192. The Cybersecurity Workforce Assessment Act, Pub. L. No. 113–246, *supra* note 8.
193. *Id.*
194. *Id.*
195. The Border Patrol Agent Pay Reform Act of 2014, Pub. L. No. 113–277, *supra* note 9.
196. *Id.*

established for such employees."[197]

F. The Cybersecurity Enhancement Act of 2014

The Cybersecurity Enhancement Act of 2014 was signed into law by the President on December 18, 2014 and provides: in Title I, a Public-Private Collaboration on Cybersecurity; Title II, Cybersecurity Research and Development; Title III, Education and Workforce Development; Title IV, Cybersecurity Awareness and Preparedness; and Title V: Advancement of Cybersecurity Technical Standards.[198] The Provisions of Title I "permit the Secretary of Commerce, acting through the Director of the National Institute of Standards and Technology (NIST), to facilitate and support the development of a voluntary, consensus-based, industry-led set of standards and procedures to cost-effectively reduce cyber risks to critical infrastructure."[199] More particularly, the law requires the Director to

> (1) coordinate regularly with, and incorporate the industry expertise of, relevant private sector personnel and entities, critical infrastructure owners and operators, sector coordinating councils, Information Sharing and Analysis Centers, and other relevant industry organizations; (2) consult with the heads of agencies with national security responsibilities, sector-specific agencies, state and local governments, governments of other nations, and international organizations; (3) identify a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, that may be voluntarily adopted by owners and operators of critical infrastructure to help identify, assess, and manage cyber risks; and (4) include methodologies to mitigate impacts on business confidentiality, protect individual privacy and civil liberties, incorporate voluntary consensus standards and industry best practices, align with international standards, and prevent duplication of regulatory processes.[200]

Title II requires that a federal cybersecurity research and development strategic plan be developed and updated every four years by the Departments of Agriculture; Commerce; Defense; Education; Energy; Health and Human Services; Interior; EPA; NASA; National Science Foundation; and other agencies considered appropriate.[201] Title II also directs that agencies "build upon existing programs to meet cybersecurity objectives, such as how to: (1) guarantee individual privacy, verify third-party software and hardware, and address insider threats; (2) determine the origin of messages transmitted over the Internet; and (3) protect information stored using cloud computing or

197. *Id.* § 226(b)(2)(A).

198. The Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274, *supra* note 10.

199. Summary: S. 1353—113th Congress (2013–2014), LIBR. OF CONG., https://www.congress.gov/bill/113th-congress/senate-bill/1353.

200. *Id.*

201. *Id.*

transmitted through wireless services."[202] Other key provisions of Title II permit the National Science Foundation to "support cybersecurity research and to review cybersecurity test beds [and] . . . if it determines that additional test beds are necessary, to award grants to institutions of higher education or research and development nonprofit institutions to establish such additional test beds."[203] National Science Foundation research and development grants are also provided for in this legislation to

> (1) secure fundamental protocols that are integral to inter-network communications and data exchange; (2) secure software engineering and software assurance; (3) holistic system security to address trusted and untrusted components, reduce vulnerabilities proactively, address insider threats, and support privacy; (4) monitoring, detection, mitigation, and rapid recovery methods; and (5) secure wireless networks, mobile devices, and cloud infrastructure.[204]

VII. CRAFTING EFFECTIVE CYBER POLICY

Until December 2014, in the absence of any U.S. legislation since 2002,[205] actions taken by the Obama administration have been focused on dealing with crisis environment near-term needs, such as "preventing cyber-based disasters and espionage, reducing impacts of successful attacks, improving inter- and intrasector collaboration, clarifying federal agency roles and responsibilities, and fighting cybercrime. However, those needs exist in the context of more difficult long-term challenges relating to design, incentives, consensus, and environment (DICE) . . . ."[206] Shackelford and Kastelic examine the NATO and European Community (EU) collection of long-term cyber strategic plans of the thirty-four (G34) nations (including the United States) having national cybersecurity strategies.[207] An analysis of these documents reveals that: (1) consistent terminology is lacking; (2) domestic cyber issues tend to be explored without consideration of global trends; (3) strategies appear vague; (4) general lack of focus on necessary education and "awareness-raising initiatives"; and (5) may fail to be "well-positioned to keep pace with rapidly advancing technology."[208]

Professor Julie Ryan contends that a number of serious geopolitical questions must be considered, including what specific cyberspace conduct "rise[s] to the level of [an] act of armed aggression? Does it matter if these acts are carried out by nations, corporations, ad hoc groups, or individuals? . . . Are the asymmetries associated with information warfare so great that unleashing the potential might in fact redraft the geopolitical landscape?"[209]

---

202. *Id.*
203. *Id.*
204. *Id.*
205. *See* Kominsky, *supra* note 3 (explaining lack of Congressional enactments relating to cybersecurity since 2002).
206. Fischer, *supra* note 39, at 6.
207. Shackelford & Kastelic, *supra* note 4, at 6.
208. *Id.* at 35.
209. JULIE RYAN ET AL., LEADING ISSUES IN INFO. WARFARE AND SEC. RES., xii (2012).

Despite whether their policies toward the Internet are characterized as "open or closed," governments worldwide continue to face "inherent perpetual difficulty in regulating online spaces."[210] Robert Faris and Rebekah Heacock Jones observe that during the past decade all governmental

> [C]ore regulatory challenges have changed in degree but not in kind; issues of scale, jurisdiction, and attribution, which are tied to the ability to conduct surveillance, complicate any efforts to regulate online activity. The ability to identify individuals associated with online activity facilitates regulation . . . and mechanisms that allow individuals to cloak their identity or to take refuge outside of their government's jurisdiction reduce regulatory effectiveness.[211]

Since 2002, Congress has needed to clarify the future roles of many agencies with respect to cybersecurity and to establish levels of funding for various cybersecurity-related activities.[212] Government policy should now be focused with laser-like precision toward achieving technological advantage. Robert D. Atkinson and David D. Castro observe that "innovation has become an important component because success in many policy areas, including health care, national defense, homeland security, transportation, energy, environment, law enforcement, and, of course, the economy, may largely be determined by our ability to develop and deploy information technology (IT)."[213]

Professor Eric Jensen argues that "three overriding problems in U.S. cybersecurity policymaking persist: (1) an overreliance on voluntary efforts to safeguard CNI [critical national infrastructure]; (2) an overly reactive focus; and (3) inadequate attention being paid to the DOD's role in prosecuting a cyber war."[214] The Congressional Research Service has described recent unsuccessful proposals and major immediate legislative needs in the categories of: information sharing between the government and private sector; FISMA reform; R&D topics and funding; cybersecurity workforce skills and preparation; protecting privately-held critical infrastructure; data-breach notification; and cybercrime law policies.[215] Several of the laws passed during December 2014 address some of these needs.[216] However, "none of these laws addresses some of the more contentious and partisan cybersecurity issues—namely, private-sector mandates, liability limitations to protect private-sector organizations that share cybersecurity-related information with government, a federal breach notification scheme, etc."[217] As has already been observed,

---

210. Robert Faris & Rebekah Heacock Jones, *Platforms and Policy*, *in* INTERNET MONITOR 2014: REFLECTIONS ON THE DIGITAL WORLD 28, 29 (Urs Gasser et al. eds., 2014).

211. *Id.*

212. *See* Kominsky, *supra* note 3 (explaining lack of Congressional enactments relating to cybersecurity since 2002).

213. Robert D. Atkinson & Daniel D. Castro, *A Nat'l Technological Agenda for the New Admin.,* 11 YALE J.L. & TECH. 190 (2009).

214. Shackelford & Kastelic, *supra* note 4 at 14 (citing Jensen, *supra* note 11, at 1561).

215. Fischer, *supra* note 39, at 5.

216. *Id.*

217. Nandini Iyer & Gabriel Ledeen, *President Signs End-of-Year Cybersecurity Legis. into Law*, JONESDAY (Dec. 2014), http://thewritestuff.jonesday.com/rv/ff001c6cee0c5cc639d89699c54c8f9176bbe492.

"[w]e cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy."[218]

A. Early 2015

On February 13, 2015, the Obama administration hosted a summit at Stanford University to coordinate private and public sector efforts aimed at enhancing the security of American consumers and businesses from cyber attack.[219] Both the U.S. Senate and House of Representatives recognize the necessity for additional cyber legislation, "[t]o improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats."[220] As this article goes to press, the Senate Intelligence Committee's Cybersecurity Information Sharing Act (CISA) finds companion legislation being crafted in the House.[221] Accordingly, "CISA would provide legal liability protection for companies sharing cyber threat data with the government. It's been a top legislative priority for many industry groups, lawmakers and government officials, who argue such an exchange is needed to prop up the nation's faltering cyber defenses."[222]

Andrew H. Tannenbaum, Cybersecurity Counsel for IBM, explains it this way, "The main reason information sharing legislation is needed is to provide legal clarity and protection for companies that seek to better protect their own networks or help other potential victims through the sharing of threat indicators."[223] As might be expected, information sharing legislation is needed

> [B]ecause current law largely consists of a patchwork of older statutes that were not written with the cyber threat in mind. Combined with the rapidly evolving nature of cybersecurity, this has led to an uncertainty among some companies about what they are permitted to do to protect their networks and to assist others in doing the same.
>
> Updating federal law to provide legal clarity and protection against frivolous lawsuits will encourage many more companies to share threat information. Such a result will benefit everyone by helping make American industry more cyber secure. Similar liability protections exist in current privacy statutes for other lawful activities, and the same clarity should be provided for valid cyber defense activities.
>
> In addition to being able to rely on appropriately tailored

218. Barack Obama, President of the United States of America, State of the Union Address (Feb. 12, 2013), http://www.whitehouse.gov/the-press-office/2013/02/12/remarks-president-state-union-address.

219. Barack Obama, U.S. President, Remarks by the President at the Cybersecurity and Consumer Protection Summit (Feb. 13, 2015), http://www.whitehouse.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit.

220. Cybersecurity Info. Sharing Act of 2014, S. 2588, 113th Cong. (2014); Lawrence J. Trautman, *Cong. Cybersecurity Oversight: Who's Who and How it Works* (forthcoming).

221. Cory Bennett, *House Intel Panel Closing in on Cyber Bill*, THE HILL (Mar. 19, 2015, 11:44 AM), http://thehill.com/policy/cybersecurity/236268-house-intel-panel-closing-in-on-cyber-bill.

222. *Id.*

223. Tannenbaum, *supra* note 76, at 4.

> authorizations for network defense activities and the sharing of threat information, companies need to be assured that information shared voluntarily will be protected from disclosures that are not authorized by the sharing entity. Companies must be able to control when and with whom their information is shared, so that they can protect their proprietary data, preserve legal safeguards such as attorney-client privilege and trade secret protections, and prevent premature public disclosure of security vulnerabilities that could put companies at greater risk.
>
> To encourage companies to share cyber threat indicators that could expose weaknesses in their networks, legislation must preclude government agencies from turning around and using the voluntarily shared information against the companies in a regulatory or other adversarial context. Companies also will be discouraged from participating in information sharing programs and receiving larger volumes of cyber threat information if by doing so they take on additional liability risk in the form of claims that they should have taken specific actions upon receiving the information. Accordingly, reasonable protection against unfair failure to warn or act claims should be provided. Companies should also be given statutory clarity that sharing cyber threat information does not run afoul of antitrust laws.[224]

Hard decisions about offensive (deterrent) cyber policy must also be developed. In testimony before the Senate Armed Services Committee, National Security Agency Director Adm. Michael S. Rogers contends that "[w]e're at a tipping point . . . . We need to think about: How do we increase our capacity on the offensive side to get to that point of deterrence?"[225] Now is the time to take advantage of the many thoughtful discussions offered by scholars, practitioners, and lawmakers to sort out and craft effective cyber policy.[226]

---

224. *Id.* at 4–5.

225. Ellen Nakashima, *Cyber Chief: Efforts to Deter Attacks Against the U.S. are Not Working*, WASH. POST (Mar. 19, 2015), http://www.washingtonpost.com/world/national-security/head-of-cyber-command-us-may-need-to-boost-offensive-cyber-powers/2015/03/19/1ad79a34-ce4e-11e4-a2a7-9517a3a70506_story.html.

226. *See, e.g.*, Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 61 (2009) (describing internet mob mentality against minorities); David G. Delaney, *Cybersecurity and the Administrative National Security State: Framing the Issues for Federal Legislation*, 40 J. LEGIS. 251, 251 (2013–14) (noting issues for federal cybersecurity legislation in the wake of the Edward Snowden affair); Lori Fossum, *Cyber Conflict Bibliography*, (GWU Legal Studies Research Paper, 2013), http://ssrn.com/abstract=2320598 (citing the multiple papers of the scholars mentioned that have furthered the cybersecurity discussion); Michael Gervais, *Cyber Attacks and the Laws of War*, 30 BERKELEY J. INT'L L. 525 (2012) (putting cybersecurity in the context of laws of war); Afroditi Papanastasiou, Application of Int'l Law in Cyber Warfare Operations (Sept. 8, 2010), http://ssrn.com/abstract=1673785 (putting cybersecurity in the context of international law); Scott Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKELEY J. INT'L L. 192 (2009) (comparing cyber war to nuclear war); K. A. Taipale, *Cyber-deterrence*, LAW, POLICY AND TECHNOLOGY: CYBERTERRORISM, INFORMATION, WARFARE, DIGITAL AND INTERNET IMMOBILIZATION, IGI GLOBAL (2010) (noting the importance of cyber-deterrence); Matthew C. Waxman, *Self-Defense Force Against Cyber Attacks: Legal, Strategic and Political Dimensions*, 89 INT'L L. STUD. 109 (2013) (including the right of self-defense to cyber attacks).

B. The Harvard Berkman Center Cybersecurity Project

During December 2014, the Harvard Berkman Center for Internet and Society launched "the cybersecurity project [to] engage in a clean-slate evaluation of the set of responsibilities related to foreign intelligence gathering . . . expanded to include the exploitation of cybersecurity vulnerabilities."[227] With support provided by the Hewlett Foundation, the cybersecurity project is led by Jonathan Zittrain (Principal Investigator), and includes former U.S. National Counterterrorism Center Director Matt Olsen, Bruce Schneier, and Harvard Berkman faculty and staff: Urs Gasser, David O'Brien, and Rob Farris.[228] For this one-year duration endeavor, the Berkman Center states,

> In this project, we aim to identify concrete steps to clarify roles and boundaries for the intelligence community, the corporate sector, academics, non-profits, and individuals; to examine how the cybersecurity risks are conceptualized and assessed by governments and companies, particularly companies with global operations; and to rebuild legitimacy and public support for cross-sectorial cybersecurity policies and practices.
>
> Part of this effort will necessarily be focused on properly framing and defining the issue. More work is needed to develop a coherent framework for understanding cybersecurity in order to develop a systematic and holistic approach for addressing cybersecurity-related problems and the intersection of these challenges with the threats to the open Internet. We wish to cut through the thicket of competing definitions and narratives describing the contours of the issue, and to develop a common language for discussing these issues across different sectors and disciplines. The core team will iterate quickly in the first three months to develop categories and frameworks that will then focus our attention, helping us and, we hope, Hewlett to assess and evaluate alternative approaches to understanding and ameliorating problems in this space. After about three months, and with the additional intellectual horsepower of the co-chairs to be recruited, we plan to check in with our framework and related priorities that emerge from that process.
>
> While the central objective is to reconsider the role of the intelligence community in cybersecurity, we also believe that it is important to identify mechanisms to strengthen the role of civil society and academic groups, which we maintain is a prerequisite for greater coordination with government and private sector groups currently working on cybersecurity and open Internet issues.[229]

227. Berkman Ctr. for Internet & Soc., *Cybersecurity Project*, HARV., http://cyber.law.harvard.edu/research/cybersecurity# (last updated Feb. 11, 2015).

228. *Id.*

229. *Id.*

C. Hewlett Foundation Cybersecurity Policy Grants

The William and Flora Hewlett Foundation's $45 million in grants to the Massachusetts Institute of Technology (MIT), Stanford University, and the University of California, Berkeley establishes "three major new academic initiatives focused on laying the foundations for smart, sustainable public policy to deal with the growing cyber threats faced by governments, businesses, and individuals."[230] As the largest financial commitment of its kind to date ($64 million total over five years), "the new programs embody campus-wide efforts to connect scholars across disciplines—including engineering, political science, economics, public policy, business, anthropology, information technology, and more—to work collaboratively on cybersecurity and policy problems."[231] The vision contemplated by the Hewlett Foundation grants contemplates diverse and complimentary roles for the new center at each school.[232] For example, the focus at MIT will be "on establishing quantitative metrics and qualitative models to help inform policymakers. Stanford's . . . extensive experience with multidisciplinary, university-wide initiatives [will] focus on the core themes of trustworthiness and governance of networks. And UC Berkeley . . . will be organized around assessing the possible range of future paths 'cybersecurity' might take."[233] Hewlett Foundation President and former Dean of the Stanford Law School, Larry Kramer says "[c]hoices we are making today about Internet governance and security have profound implications for the future . . . . To make those choices well, it is imperative that they be made with some sense of what lies ahead and, still more important, of where we want to go."[234]

D. Massachusetts Institute of Technology (MIT) Cybersecurity Policy Initiative

The Massachusetts Institute of Technology (MIT) Cybersecurity Policy Initiative (CPI) seeks to form a scholarly foundation based on three interdisciplinary pillars: Engineering, social science, and management. Engineering is vital to understanding the architectural dynamics of the digital systems in which risk occurs. Social science can help explain institutional behavior and frame policy solutions, while management scholars offer insight on practical approaches to institutionalize best practices in operations."[235] Daniel Weitzner is a principal research scientist at MIT's Computer Science

230. *Hewlett Foundation Announces $45 Million in Grants to MIT, Stanford, UC Berkeley to Establish Major New Academic Centers for Cybersecurity Policy Research*, THE WILLIAM AND FLORA HEWLETT FOUND. (Nov. 18, 2014), http://www.hewlett.org/newsroom/press-release/hewlett-foundation-announces-45-million-grants-mit-stanford-uc-berkeley-establish-major-new-academic.

231. *Id.*

232. *Id.*

233. *Id.*

234. Clifton B. Parker, *Stanford Cyber Initiative Will Tackle Internet Technology Concerns From Many Angles*, STAN. REP. (Nov. 18, 2014), http://news.stanford.edu/news/2014/november/cyber-security-initiative-111814.html.

235. *Hewlett Foundation Funds New MIT Initiative on Cybersecurity Policy*, MIT News (Nov. 18, 2014), http://newsoffice.mit.edu/2014/hewlett-foundation-funds-mit-initiative-cybersecurity-policy-1118.

and Artificial Intelligence Laboratory (CSAIL) and serves as the principal investigator for the MIT Cybersecurity Policy Initiative.[236] Weitzner states, "[w]e're very good at understanding the system dynamics on the one hand, then translating that understanding into concrete insights and recommendations for policymakers. And we'll bring that expertise to the understanding of connected digital systems and cybersecurity. That's our unique contribution to this challenge."[237] Professor Weitzner was the White House's United States deputy chief technology officer for internet policy from 2011 to 2012, and observes,

> Developing a more formal understanding of the security behavior of large-scale systems is a crucial foundation for sound public policy. As an analogy, imagine trying to shape environmental policy without any way of measuring carbon levels in the atmosphere and no science to assess the cost or effectiveness of carbon mitigation tools. This is the state of cybersecurity policy today: growing urgency, but no metrics and little science. CSAIL is home to much of the technology that is at the core of cybersecurity, such as the RSA cryptography algorithm that protects most online financial transactions, and the development of web standards via the MIT-based World Wide Web Consortium. That gives us the ability to have our hands on the evolution of these technologies to learn about how to make them more trustworthy.[238]

MIT's Cryptography and Information Security Group of the Computer Science and Artificial Intelligence Laboratory (CSAIL) include Professors: Shafi Goldwasser; Butler Lampson; Silvio Micali; Ronald L. Rivest; and Vinod Vaikuntanathan.[239] Nir Bitansky and Abishek Jain are also major contributors in this area.[240] Professor Nickolai Zeldovich leads the Computer Systems Security Group, where Haogang Chen contributes.[241]

E. Southern Methodist University Darwin Deason Institute For Cyber Security

At Southern Methodist University (SMU), the mission of the Darwin Deason Institute for Cyber security is to "advance the science, policy, application and education of cyber security through basic and problem-driven, interdisciplinary research. The Institute is committed to the goal of emerging as a world-class cybersecurity research center that innovates, develops and delivers solutions to the nation's most challenging cyber security problems."[242]

---

236. *Id.*
237. *Id.*
238. *Id.*
239. *CIS Members*, MIT THEORY OF COMPUTATION, http://toc.csail.mit.edu/cis_members (last visited Sept. 22, 2015).
240. *Id.*
241. *MIT CSAIL Computer Systems Security Group*, MIT, http://css.csail.mit.edu/ (last visited Aug. 27, 2015).
242. *About the Darwin Deason Institute for Cyber Security*, SMU LYLE INSTITUTES, http://www.smu.edu/Lyle/Institutes/DeasonInstitute/AboutInstitute (last visited Sept. 22, 2015).

The Institute, under the direction of Frederick R. Chang, consists of four substantive programs: Hardware and network security engineering; software and systems security; economics and social sciences; and policy and law.[243] Professor Chang, a recognized national expert in cybersecurity, is the former Director of Research at the National Security Agency, served as a member of the Commission on Cyber Security for the 44th Presidency, and served as a member of the Computer Science and Telecommunications Board of the National Academies.[244]

F. Stanford Cyber Initiative

Stanford University's Cyber Initiative is intended to "be highly interdisciplinary in building a new policy framework for cyber issues. It will draw on the campus' experience with multidisciplinary, university-wide initiatives to focus on the core themes of trustworthiness, governance and the emergence of unexpected impacts of technological change over time."[245] Stanford President John Hennessey says, "[o]ur increasing reliance on technology, combined with the unpredictable vulnerabilities of networked information, pose future challenges for all of society . . . Stanford has a long history of fostering interdisciplinary collaborations to find thoughtful and enlightened answers to these paramount questions."[246]

Former Stanford Professor Mariano-Florentino Cuéllar (now Associate Justice on the California Supreme Court) is credited with leading the planning effort for Stanford's Cyber Initiative.[247] Others in the multidisciplinary effort include: Roberta Katz (Strategic Advisor and Stanford's Office of the President); Megan Pierson (Senior University Counsel); John Mitchell (computer science and engineering); Jeremy Bailenson (communications); Stephen Barley (management science and engineering); Dan Boneh (computer science and electrical engineering); Ian Morris (classics and history); Barbara van Schewick (law); Amy Zegart (Hoover Institution); George Triantis (law and Assoc. Dean of Research); and Allison Berke (operations).[248]

G. University of California, Berkeley's Center for Long-Term Cybersecurity

The Cyber Initiative at UC Berkeley "is intended to foster the development of policy frameworks to help guide sustainable solutions, to develop trust and improve communication among the disparate actors, and to provide scholars and practitioners with needed technological and policy

243. *Id.*; *see also About the Director*, SOUTHERN METHODIST UNIVERSITY LYLE INSTS., http://www.smu.edu/Lyle/Institutes/DeasonInstitute/AboutDirector (last visited Aug. 27, 2015) (introducing Frederick R. Chang).

244. *Id.*

245. Clifton B. Parker, *Stanford Cyber Initiative Will Tackle Internet Technology Concerns From Many Angles*, STANFORD NEWS (Nov. 18, 2014), http://news.stanford.edu/news/2014/november/cyber-security-initiative-111814.html.

246. *Id.*

247. *Id.*

248. *See id.* (listing committee members).

expertise."[249] UC Berkeley Chancellor Nicholas Dirks says, "[o]ur faculty at Berkeley are perfectly suited to help lead the way in pursuing independent scholarship in this field, and we are delighted to partner on this with the Hewlett Foundation and our great peer universities."[250] Dean AnnaLee Saxenian of UC Berkeley's School of Information says "the [Information] School's faculty spans the fields of law and policy, computer science and engineering, and the social and behavioral sciences, so we are ideally positioned to advance our thinking about the long-term future of cybersecurity."[251] UC Berkeley Professor Steven Weber states, "[t]he goal of Berkeley's new Center for Long-Term Cybersecurity is first to map out what the cybersecurity problem itself will come to mean a few years hence, and then to generate and facilitate the forward looking, interdisciplinary research efforts that will make a difference."[252]

Additional faculty leadership for the UC Berkeley's School of Information's (I-School), Center for Long-term Cybersecurity include: John Chuang (I-School); Deirdre Mulligan (I-School); and Douglas Tygar (Computer Science & I-School). Affiliated faculty include: Kenneth A. Bamberger (Law & Co-Director, Berkeley Center for Law and Technology); Chris Jay Hoofnagle (Director, Berkeley Center for Law and Technology, Information Privacy Program); Anthony C. Joseph (Computer Science); Stephen Maurer (Director, IT & Homeland Security Project, School of Public Policy); Michael Nacht (School of Public Policy); Vern Paxson (Computer Science); and S. Shankar Sastry (Dean, College of Engineering).[253]

H. National Centers of Academic Excellence in Information Assurance / Cyber Defense

The first fourty-four designated academic institutions as NSA/DHS National Centers of Academic Excellence (CAE) in information Assurance (IA)/Cyber Defense are "based on updated academic criteria for Cybersecurity education and affords each CAE institution the opportunity to distinguish its strengths in specific IA/CD focus areas."[254] Intended to help educate and provide for trained professionals to meet the growing need to reduce vulnerabilities in the nation's networks, NSA started this program in 1998, with DHS joining as a partner in response to the President's National Strategy to Secure Cyberspace during 2004.[255] By 2008, a Center of Academic

249. Kathleen Maclay, *$45 Million in Grants Fund New Cybersecurity Centers at UC Berkeley, MIT and Stanford*, BERKELEY NEWS (Nov. 18, 2014), http://newscenter.berkeley.edu/2014/11/18/45-million-in-grants-fund-new-cybersecurity-centers-at-uc-berkeley-mit-and-stanford/.

250. *Id.*

251. *Id.*

252. *Id.*

253. *Center for Long-Term Cybersecurity*, UC BERKELEY SCH. OF INFO., http://www.ischool.berkeley.edu/cltc (last updated Mar. 26, 2015).

254. *National Centers of Academic Excellence in Information Assurance (IA)/Cyber Defense (CD)*, NAT. SEC. AGENCY/CENT. SEC. SERV., https://www.nsa.gov/ia/academic_outreach/nat_cae/ (last updated Aug. 20, 2014).

255. *Id.*

Excellence program in Information Assurance (IA) is added, "to encourage universities and students to pursue higher-level doctoral research in Cybersecurity;" and, a two-year institution and technical school program during 2010.[256] A list of institutions designated to date as National Centers of Academic Excellence in Information Assurance (IA) / Cyber Defense (CD) is presented in the Appendix to this article.

I. Washington, D.C Area Academic Community

Proximity to much of the nation's cyber infrastructure—National Security Agency (NSA), U.S. Cyber Command, and the NIST may account for many nearby educational institutions growing to play a major role in developing academic programs to meet the critical need for cyber skills. Particularly noteworthy are programs at Towson University, the University of Maryland (Baltimore County), University of Maryland University College, University of Maryland (College Park), and Virginia Polytechnic and State University.[257]

George Mason University's Center for Secure Information Systems (CSIS), established in 1990, claims the distinction of being the first academic center in security at a U.S. university.[258] Under the direction of Sushil Jajodia, other CSIS faculty include: Massimiliano Albanese (applied information technology); Kai Zeng (electrical and computer engineering); Alexander H. Levis (systems architecture); Rajesh Ganesan (systems engineering and operations research); and Lieutenant General Robert Elder (USAF, retired).[259] The George Mason University course catalog states

> Cyber Security Engineering is concerned with the sustainability of today's systems which depend not just on protecting computers and networks; it requires a proactive approach in engineering design of physical systems with cyber security incorporated from the beginning of system development. Cyber security engineering is an important quantitative methodology to be used in all industries to include, but not limited to, transportation, energy, healthcare, infrastructure, finance, government (federal, state, and local), and defense. The program is focused on the cyber security engineering of integrated cyber-physical systems.[260]

Also making significant contributions issues impacting cybersecurity is George Mason's Mercatus Center, which describes their objective as to advance "knowledge about how markets work to improve people's lives by training graduate students, conducting research, and applying economics to

256. *Id.*

257. *Id.*

258. *Welcome to CSIS, Center for Secure Information Systems*, GEO. MASON U., http://csis.gmu.edu/index.php (last visited Sept. 22, 2015).

259. *See Faculty, Center for Secure Information Systems*, GEO. MASON U., http://csis.gmu.edu/pages/faculty.php (last visited Sept. 22, 2015) (introducing the members of the Center for Secure Information Systems faculty).

260. *Cyber Security Engineering, BS*, GEO. MASON U., http://catalog.gmu.edu/preview_program.php (last visited Sept. 22, 2015).

offer solutions to society's most pressing problems."[261] Economics Professor Tyler Cowan is the current faculty director; with significant technology contributions made by Adam D. Thierer, Jerry Brito, and Eli Dourado.[262]

VIII. CONCLUSION

Cybersecurity vulnerability has the potential to be the "ultimate weapon" used against the United States. Here, a brief description is presented about how selected U.S. constituencies view their likely capabilities to defend against cyberthreat. Much like fighting the Ebola virus, any effective policy requires leadership and coordination by the Federal government. Taking note of the five cybersecurity-related bills signed into law during December 2014, the first cybersecurity legislation enacted since 2002, policy developments to date are then examined. From the standpoint of aggregate cost to society, the U.S. national security infrastructure is the only institutional framework capable of effectively protecting the American public from cyberattack. Much like an Ebola outbreak or traditional war, cybersecurity policy needs to be recognized as a response to the crisis it is; cyberthreat is responsible for profound economic disruption and has the capacity to end human life on a wholesale basis. The time for effective and comprehensive cybersecurity policy is now.

261. *About*, MERCATUS CTR. GEO. MASON U., http://mercatus.org/content/about (last visited Sept. 22, 2015).

262. *Id.*; Jerry Brito & Tate Watkins, *Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy*, 3 HARV. NAT'L SEC. J. 39, 39 (2012); Eli Dourado & Andrea Castillo, *Why the Cybersecurity Framework Will Make Us Less Secure*, MERCATUS CTR. AT GEO. MASON U. (Apr. 17, 2014), http://mercatus.org/sites/default/files/Dourado_CybersecurityFramework_v2.pdf; Sean Lawson, *Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats*, 10 J. INFO. TECH. & POL. (2013).

IX. APPENDIX

National Centers of Academic Excellence in Information Assurance (IA) / Assurance Research (R)

Four-Year Education and Research:
Air Force Institute of Technology (Ohio) (IA) (R)
Arizona State University (Arizona) (IA) (R)
Auburn University (Alabama) (IA) (R)
Bellevue University (Nebraska) (IA)
Boston University (Massachusetts) (IA) (R)
Bowie State University (Maryland) (IA)
Brigham Young University (Utah) (IA)
California State Polytechnic University, Pomona (California) (IA)
California State University, Sacramento (California) (IA)
California State University, San Bernardino (California) (IA)
Capella University (Minnesota) (IA)
Capitol College (Maryland) (IA)
Carnegie Mellon University (Pennsylvania) (IA) (R)
Champlain College (Vermont) (IA)
Clark Atlanta University (Georgia) (IA)
Colorado Technical University (IA)
Columbus State University (Georgia) (IA)
Dakota State University (South Dakota) (IA)
Dartmouth College (New Hampshire) (R)
Davenport University (Michigan) (IA)
DePaul University (Illinois) (IA)
Drexel University (Pennsylvania) (IA)
East Carolina University (North Carolina) (IA)
East Stroudsburg University of Pennsylvania (IA)
Eastern Michigan University (Michigan) (IA)
Fairleigh Dickinson University (New Jersey) (IA)
Ferris State University (Michigan) (IA)
Florida A&M University (Florida) (IA)
Florida Atlantic University (Florida) (R)
Florida Institute of Technology (Florida) (R)
Florida State University (IA) (R)
Fort Hayes State University (Kansas) (IA)
Fountainhead College of Technology (Tennessee) (IA)
George Mason University (Virginia) (IA) (R)
Georgetown University (Washington, DC) (IA)
Georgia Institute of Technology (Georgia) (R)
Hampton University (Virginia) (IA)
Howard University (Washington, DC) (IA)
Idaho State University (Idaho) (IA)
Illinois Institute of Technology (Illinois) (IA)
Illinois State University (Illinois) (IA)

Indiana University of Pennsylvania (IA)
Information Resources Management College (Washington, DC) (IA)
Iowa State University (Iowa) (IA) (R)
Jacksonville State University (Alabama) (IS)
James Madison University (Virginia) (IA)
Jersey City University (New Jersey) (IA)
Johns Hopkins University (Maryland) (IA) (R)
Kansas State University (Kansas) (R)
Kennesaw State University (Georgia) (IA)
Lewis University (Illinois) (IA)
Louisiana Tech University (Louisiana) (IA)
Manhattan Area Technical College (Kansas) (R)
Marymount University (Virginia) (IA)
Mercy College (New York) (IA)
Metropolitan State University (Minnesota) (IA)
Mississippi State University (Mississippi) (IA) (R)
Missouri University of Science and Technology (Missouri) (IA) (R)
National University (California) (IA)
Naval Postgraduate School (California) (IA) (R)
New Mexico Tech (New Mexico) (IA) (R)
New Jersey Institute of Technology (New Jersey) (IA)
New York University (New York) (R)
Norfolk State University (Virginia) (IA)
North Carolina A&T State University (North Carolina) (IA)
North Carolina State University (North Carolina) (R)
Northeastern University (Massachusetts) (IA) (R)
Norwich University (Vermont) (IA)
Nova Southeastern University (Florida) (IA)
Ohio State University (Ohio) (IA)
Oklahoma State University (Oklahoma) (IA) (R)
Our Lady of the Lake University (Texas) (IA)
Pace University (New York) (IA)
Polytechnic University (New York) (IA) (R)
Polytechnic University of Puerto Rico (Puerto Rico) (IA)
Princeton University (New Jersey) (R)
Purdue University (Indiana) (R)
Regis University (Colorado) (IA)
Rice University (Texas) (R)
Rochester Institute of Technology (New York) (IA)
Rutgers University (New Jersey) (IA) (R)
Southern Illinois University Carbondale (Illinois) (IA)
Southern Methodist University (Texas) (IA)
Southern Polytechnic State University (Georgia) (IA)
St. Cloud State University (Minnesota) (IA)
Syracuse University (New York) (IA) (R)
Texas A&M University (IA) (R)
Texas A&M University- Corpus Christi (IA)

Texas A&M University- San Antonio (IA)
The George Washington University (Washington, DC) (IA) (R)
The Pennsylvania State University (Pennsylvania) (IA) (R)
The University of Alabama at Birmingham (Alabama) (R)
The University of Alabama at Huntsville (Alabama) (IA)
The University of Arizona, Tucson (Arizona) (IA)
The University of Texas at San Antonio (Texas) (IA) (R)
The University of the District of Columbia (Washington, DC) (IA)
Towson University (Maryland) (IA)
Tuskegee University (Alabama) (IA)
United States Air Force Academy (Colorado) (IA)
United States Military Academy, West Point (New York) (IA)
United States Naval Academy (Maryland) (IA)
University of Advancing Technology (Arizona) (IA)
University of Alaska Fairbanks (IA)
University of Arkansas (Arkansas) (R)
University of Arkansas at Little Rock (Arkansas) (IA)
University of Arizona, Tucson (Arizona) (IA)
University of Buffalo, the State University of New York (IA) (R)
University of California, Davis (California) (IA) (R)
University of California, Irvine (California) (R)
University of Colorado (Colorado Springs) (IA)
University of Connecticut (Connecticut) (R)
University of Dallas (Texas) (IA)University of Denver (Colorado) (IA)
University of Detroit, Mercy (Michigan) (IA)
University of Houston (Texas) (IA)
University of Idaho (Idaho) (IA)
University of Illinois at Urbana-Champaign) (IA) (R)
University of Illinois at Springfield (Illinois) (IA)
University of Kansas (Kansas) (IA)
University of Maryland, Baltimore County (Maryland) (IA) (R)
University of Maryland, College Park (Maryland) (R)
University of Maryland University College (Maryland) (IA)
University of Massachusetts (Amherst) (IA) (R)
University of Memphis (Tennessee) (IA) (R)
University of Minnesota (Minnesota) (IA)
University of Missouri- Comumbia (Missouri) (IA)
University of Nebraska at Omaha (Nebraska) (IA)
University of Nevada, Las Vegas (Nevada) (IA)
University of New Mexico (New Mexico) (IA) (R)
University of New Orleans (Louisiana) (R)
University of North Carolina at Charlotte (North Carolina) (IA) (R)
University of North Texas (Texas) (IA)
University of Pittsburgh (Pennsylvania) (IA) (R)
University of Rhode Island (IA) (R)
University of South Alabama (Alabama) (IA)
University of South Carolina (South Carolina) (IA)

University of Southern California (California) (R)
University of Tennessee at Chattanooga (Tennessee) (IA)
University of Texas at Austin (Texas) (R)
University of Texas at Dallas (Texas) (IA) (R)
University of Texas at El Paso (Texas) (IA)
University of Tulsa (Oklahoma) (IA) (R)
University of Washington (Washington) (IA) (R)
Utica College (Newly designated CAE) (New York)
Virginia Polytechnic and State University (Virginia) (R)
Walsh College (Michigan) (IA)
West Chester University of Pennsylvania (IA)
West Virginia University (West Virginia) (IA) (R)
Wilmington University (Delaware) (IA)
Worcester Polytechnic Institute (Massachusetts) (R)

CAE IA/CD Focus Areas:
California State University, San Bernardino (California)
Cyber Investigations
Network Security Administration
The University of Texas at San Antonio (Texas)
Digital Forensics

Two-Year Education:
Anne Arundel Community College (Maryland)
Blue Ridge Community and Technical College (West Virginia)
Bossier Parish Community College (Louisiana)
College of Southern Maryland (Maryland)
Erie Community College (New York)
Florida State College at Jacksonville (Florida)
Francis Tuttle Technology School (Oklahoma)
Hagerstown Community College (Maryland)
Harford Community College (Maryland)
Highline Community College (Washington)
Honolulu Community College (Hawaii)
Howard community College (Maryland)
Inver Hills Community College (Minnesota)
Ivy Tech Community College (Indiana)
Jackson State Community College (Tennessee)
Minneapolis Community and Technical College (Minnesota)
Montgomery College (Maryland)
Moraine Valley Community College (Illinois)
Northern Virginia Community College (Virginia)
Oklahoma City Community College (Oklahoma)
Oklahoma Department of Career & Technology (Oklahoma)
Owens Community College (Ohio)
Prince George's Community College (Maryland)

Richland College of the Dallas County Community College Dist. (Texas)
Rose State College (Oklahoma)
San Antonio College (Texas)
Sinclair Community College (Ohio)
Snead State Community College (Alabama)
St. Phillip's College (Texas)
The Community College of Baltimore County (Maryland)
Valencia College (Florida)
Watcom Community College (Washington)

Source: Nat'l Sec. Agency/Cent. Sec. Serv., Nat'l Ctrs. of Acad. Excellence in Info. Assurance (IA)/Cyber Def. (CD) (Aug. 20, 2014), https://www.nsa.gov/ia/academic_outreach/nat_cae/; Nat'l Sec. Agency/ Cent. Sec. Serv., Nat'l Ctrs. of Acad. Excellence in Info. Assurance (July 29, 2014), https://www.nsa.gov/ia/academic_outreach/nat_cae/institutions.shtml (last visited Sept. 22, 2015).