MERCATUS ON POLICY

"Information Sharing": No Panacea for American Cybersecurity Challenges

Eli Dourado and Andrea Castillo

June 2015

MERCATUS CENTER
George Mason University

Eli Dourado is a research fellow at the Mercatus Center at George Mason University and director of its Technology Policy Program. He specializes in Internet governance, intellectual property, cryptocurrency, Internet security, and the economics of technology. His popular writing has appeared in the *New York Times*, the *Washington Post*, *Foreign Policy*, the *Guardian*, *Ars Technica*, and *Wired*, among other outlets. Dourado is a member of the State Department's International Telecommunication Advisory Committee and has served on several US delegations to UN treaty and policy conferences. In 2013, he won an IP3 award from Public Knowledge for the creation of WCITLeaks .org, a transparency website focused on the UN's International Telecommunication Union. Dourado is a PhD candidate in economics at George Mason University and received his BA in economics and political science from Furman University.

Andrea Castillo is the program manager of the Technology Policy Program for the Mercatus Center at George Mason University and is pursuing a PhD in economics at George Mason University. She is a coauthor of *Liberalism and Cronyism: Two Rival Political and Economic Systems* with Randall G. Holcombe and *Bitcoin: A Primer for Policymakers* with Jerry Brito. Castillo received her BS in economics and political science from Florida State University.

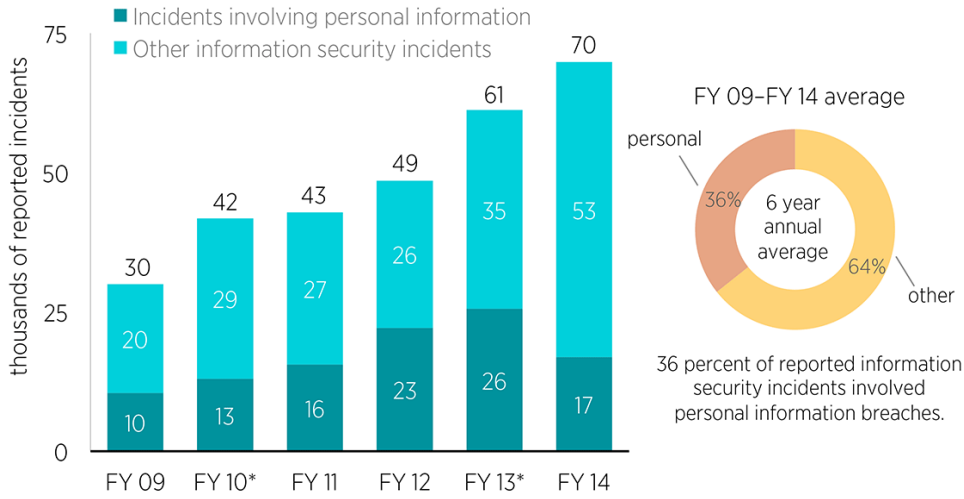
As the number and cost of information security incident failures continue to rise,[1] the federal government is considering legislative responses to address national cybersecurity vulnerabilities. Federal proposals from the executive and legislative branches emphasize increasing "information sharing" about cyberthreats among private and public entities to improve system preparedness. However, preexisting government, public-private, and private sector information sharing initiatives have not succeeded at preventing cyberattacks as proponents of these initiatives allege. Additionally, longstanding federal information security weaknesses render the federal government an especially poor candidate to manage large amounts of sensitive private data, as the recent massive information breach of the Office of Personnel Management (OPM) demonstrates.[2]

After briefly outlining the current cybersecurity information sharing proposals, we will examine the performance of the many similar programs that the federal government has operated for years. The government's inability to properly implement previous information sharing systems even internally, along with its ongoing failures to secure its own information systems, casts doubt on the viability of proposed government-led information sharing initiatives to improve the nation's cybersecurity. We will then examine the flawed assumptions that underlie information sharing advocacy before exploring solutions that can comprehensively address the nation's cybersecurity vulnerabilities.

WHAT DO INFORMATION SHARING INITIATIVES PROPOSE?

The premise behind cyberthreat information sharing initiatives is that network administrators who notice a new kind of attack or vulnerability can help others

FIGURE 1. SHARE OF REPORTED FEDERAL INFORMATION SECURITY INCIDENTS INVOLVING PERSONAL INFORMATION.



Data note: OMB calculation methodologies of total Federal Information Security Management Act spending changed in indicated years. Sources: Congressional Research Service, "Cybersecurity Issues and Challenges: In Brief," December 16, 2014; Office of Management and Budget, Annual Report to Congress: Federal Information Security Management Act (Washington, DC, Febraury 2015), http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy14_fisma_report_02_27_2015.pdf. Produced by Eli Dourado, Andrea Castillo, and Rizqi Rachmat, Mercatus Center at George Mason University, March 2015.

to defend against intrusion by quickly publicizing the discovery.[3] In practice, however, private entities can be reluctant to share such threat information for several reasons, including their desires to protect customer privacy, trade secrets, or public reputation.[4] Advocates argue that the federal government can increase information sharing among entities, and therefore improve cybersecurity, by extending legal immunity to private corporations that share private customer data with federal agencies in a compliant manner.[5]

Several such proposals have been introduced this year. The House of Representatives passed the Protecting Cyber Networks Act in April of 2015, which would shield private entities that shared cyber threat indicators with federal agencies from legal action by aggrieved parties.[6] The Senate's version of an information sharing bill, the Cybersecurity Information Sharing Act (CISA), proposes similar policies.[7] On the executive level, president Obama proposed a plan to promote information sharing among private and public entities[8] and created through executive order a new Cyber Threat Intelligence Integration Center (CTIIC) to coordinate information sharing under the Director of National Intelligence (DNI).[9] The Department of Homeland Security (DHS), Department of Defense (DOD), Department of Justice (DOJ), and DNI would be empowered to receive, analyze, store, and disseminate sensitive threat data from private entities to varying degrees under each proposal. In contrast, members of the House who see protecting strong encryption as a solution to strengthen both privacy and security have passed an amendment to the Commerce, Justice, and Science appropriations bill to prevent the National Institute of Standards and Technology (NIST) from weakening encryption standards.[10] While information sharing proposals are currently intended to be voluntary, some have suggested that such initiatives will not work as intended unless made compulsory.[11] On the other hand, sharing cyberthreat information with government agencies raises concerns from privacy and civil liberties groups, even when sharing is nonmandatory.[12] Laws like CISA could open another channel for intelligence agencies to extract private data for criminal investigations completely unrelated to cybersecurity.[13]

EXISTING FEDERAL SHARING PROGRAMS HAVE NOT WORKED

Information sharing initiatives are not novel. A 1998 presidential order authorized the formation of public-private partnerships to share threat information within critical infrastructure industries.[14] Dozens of such Information Sharing and Analysis Centers (ISACs) have coordinated cyberthreat information flows among public and private entities since that time.[15] Additionally, at least 20 federal offices already

carry out missions that prioritize information sharing and public-private cybersecurity coordination.[16] The National Cybersecurity and Communications Center (NCCIC), a DHS cyberthreat coordination center, houses the US Computer Emergency Response Team (US-CERT), which has served as the primary cyberthreat collection, assistance, and notification center since it was founded in 2003. President Obama created the CTIIC in February 2015 to advance information sharing goals along with the NCCIC, the Federal Bureau of Intelligence's National Cyber Investigative Task Force, DOD's US Cyber Command, and "other relevant United States Government entities"—which could amount to several dozen offices. Such overlapping roles and unclear lines of communication results in waste, inefficiency, and poorer security outcomes.[17]

Despite the ample resources devoted to this task, the federal government has struggled to effectively collect and share incident information internally and with the private sector.[18] ISACs can cease to operate if members do not actually share valuable information.[19] A DHS Inspector General Report finds that the NCCIC faces large challenges in effectively sharing information among the appropriate parties. As of October 2014, the NCCIC had not even developed a common incident management system to coordinate information sharing—five years after being formed to do so.[20] US-CERT has yet to develop performance metrics to gauge and improve effectiveness, despite serving as the main federal cybersecurity consultant for over a decade.[21] Additionally, private sector threat analysis efforts often outpace US-CERT in breach notification.[22] Indeed, DHS has at times been unable to even adequately share threat information within its own offices. In March 2013, DHS's own US-CERT issued a warning about Windows XP vulnerabilities to government and private sector partners.[23] But by November of that year, DHS' Inspector General reported that several DHS computers were still running a vulnerable version of Windows XP, even after other DHS representatives ensured they had stopped running that version.[24]

The Congressional Research Service notes "greater information sharing may, in some instances, effectively weaken cybersecurity by creating an overwhelming amount of information, eliminating the capacity to pay attention to truly important alerts."[25] The federal government sought to overcome this challenge by developing technological tools to surveil network activity, called the "EINSTEIN" projects,[26] yet these projects often run over cost and perform worse than anticipated.[27] Indeed, the EINSTEIN projects failed to identify the recent OPM hack.[28] However ambitious their design, these programs have so far proven too technologically crude to handle the complex central identification and communication efforts intended to protect federal systems.[29] There may never be enough EINSTEINs in the world for DHS, DOD, and DOJ to adequately coordinate and respond to the massive amounts of private data that would be collected under CISA.

SYSTEMIC SECURITY WEAKNESSES PLAGUE FEDERAL SYSTEMS

Federal information sharing initiatives have proven unsuccessful in stemming the number of reported agency information security failures. These longstanding cybersecurity weaknesses and failures render the federal government a poor candidate to manage more private data as has been proposed.[30] The number of incidents reported to US-CERT increased by 1,169 percent since fiscal year (FY) 2006, reaching an all-time high of 69,851 last year.[31] Additionally, federal agencies have in general struggled to secure personally identifiable information (PII) of personnel and civilians. Almost 40 percent of the roughly 300,000 reported federal information security incidents from FY 2009 to FY 2014 involved sensitive PII being potentially exposed to outside groups.[32]

The recent OPM hack clearly highlights the dangers of entrusting massive amounts of private data to federal agency management. Recent reports reveal that, contrary to early official statements that hackers only gained a limited amount of information, the Social Security numbers and addresses of over 14 million current and former employees and contractors, including intelligence and military officials in the most need of data protection,[33] were extracted by foreign hackers. In addition, hackers accessed reams of Standard Form 86 questionnaires used for conducting background checks, which contain sensitive data about applicants' family, friends, and former coworkers.[34] Despite serving as the central human resource department for the entire federal government, OPM did not employ any security staff until 2013.[35] Much of the data was not even encrypted.[36] Early reports that the federal government's EINSTEIN threat detection system identified the breach were similarly incorrect; a product demonstration by an outside vendor reportedly first found the hack in April.[37]

Information sharing legislation could expand the circle of Americans harmed by such government breaches.

Importantly, the agencies that would be entrusted with significant new data extraction and management responsibilities under CISA reported alarming security breaches last year.[38] DOJ employees downloaded malicious software onto agency computers 182 times in FY 2014 and reported a total of 3,604 incidents for the year. Of the 2,608 reported DHS failures, employees reported 1,816 pieces of computer equipment lost or stolen. DOD personnel downloaded malware onto network systems 370 times and reported roughly 2,500 employee policy violations in the past year alone, as well as 1,758 other incidents. Additionally, each agency has suffered major system infiltrations by malicious hackers in recent years—sometimes involving sensitive data extractions by hostile external groups.[39] If these agencies' already weak information management capacities are further strained, the rate of PII exposures could ultimately increase—and even have the unintended consequence of weakening cybersecurity and increasing attacks on federal systems. Malicious hackers would, after all, know that these ill-defended agencies would be managing massive amounts of potentially valuable data, thereby creating a tempting target for infiltration.

WE NEED BETTER CYBERSECURITY SOLUTIONS

The professional information security community is accordingly skeptical that such calls for top-down, government-driven information sharing of cyberthreats will actually diminish or prevent breaches. One poll of privacy and security experts from across the government, private sector, and academia finds that 87 percent do not believe that CISA-style information sharing initiatives will "significantly reduce security breaches."[40] Some respondents replied that while information sharing may be useful on the margins, placing it as the center of a top-down, government-driven panacea to protect national networks is inadequate and even counterproductive. Others in the security community are concerned that such initiatives merely use the guise of cybersecurity to push through measures secretly intended to increase surveillance of online activity.[41]

Most agree that information sharing alone will not significantly improve cybersecurity preparedness. Industry studies find that external attacks only constitute 37 percent of reported root causes; system glitches and human error, respectively, make up 29 percent and 35 percent of the remainder.[42] This Band-Aid solution does not address the core problems of poor security practices, inadequate user education[43] and authentication requirements,[44] and proper investment in defensive technology.[45] In the worst-case scenario, high-profile information sharing measures like CISA will serve to ultimately weaken cybersecurity if they instill a false sense of security among government and private actors, leading them to neglect these other critical factors that are arguably more imperative for robust cybersecurity.[46]

This is not to say that there is nothing to be done about cybersecurity. Instead of relying on a rigid top-down plan managed by poorly secured government agencies, public and private entities should work together using a "collaborative security" approach that fosters collective responsibility, evolutionary consensus, and nested decision making.[47] Government officials should encourage, not weaken, good security practices like strong authentication and encryption.[48] Legislation that protects and encourages the use of strong encryption will do far more to promote strong cybersecurity. Federal officials should stop contradicting each other on the need for strong encryption, and encourage efforts like CIO Tony Scott's policy to require encrypted connection for all government websites. Likewise, government agencies should cease the practice of purchasing "zero-day exploits," or publicly unknown security vulnerabilities, without notifying the relevant parties of discovered system weaknesses.[49] Finally, government agencies can simultaneously improve their own system defenses and promote private sector security by purchasing cybersecurity insurance policies for their own networks and thereby stimulating this industry.[50]

ENDNOTES

1. Roughly 42.8 million cyberattacks were reported in 2014, each imposing an average of around $780,000 in costs on businesses. See: David Burg, Sean Joyce, and Mark Lobel, "Managing Cyber Risks in an Interconnected World: Key Findings from the Global State of Information Security Survey 2015" (Report, PricewaterhouseCoopers, London, September 2014), http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml; "IT Security Risks Survey 2014: A Business Approach to Managing Data Security Threats" (Report, Kaspersky Labs, Moscow, July 29, 2014), https://business.kaspersky.com/it-security-risks-survey-2014-none-is-spared/2339.

2. David Perera and Joseph Marks, "Newly Disclosed Hack Got 'Crown Jewels,'" Politico, June 12, 2015, http://www.politico.com/story/2015/06/hackers-federal-employees-security-background-checks-118954.html.

3. N. Eric Weiss, "Legislation to Facilitate Cybersecurity Information Sharing: Economic Analysis" (Report No. R43821, Congressional Research Service, Washington, DC, February 23, 2015), http://fas.org/sgp/crs/misc/R43821.pdf.

4. Andrew Nolan, "Cybersecurity and Information Sharing: Legal Challenges and Solutions" (Report No. R43941, Congressional Research Service, March 16, 2015), http://www.fas.org/sgp/crs/intel/R43941.pdf.

5. See: Weiss, "Legislation to Facilitate Cybersecurity Information Sharing"; Eric A. Fischer, "Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions" (Report No. R42114, Congressional Research Service, June 20, 2013), https://fas.org/sgp/crs/natsec/R42114.pdf.

6. Protecting Cyber Networks Act, H.R. 1560, 114th Cong. (2015).

7. Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. (2015).

8. Exec. Order No. 13691, 80 Fed. Reg. 9347 (2015).

9. White House Office of the Press Secretary, "Fact Sheet: Cyber Threat Intelligence Integration Center," February 25, 2015, https://www.whitehouse.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center.

10. "House Passes Massie Amendment to Strengthen Privacy and Security," Congressman Thomas Massie website, June 4, 2015, https://massie.house.gov/press-release/press-release-house-passes-massie-amendment-strengthen-privacy-and-security.

11. See Nathan Alexander Sales, "Regulating Cyber-Security," *Northwestern University Law Review* 107, no. 4 (2013); Jeremy J. Broggi, "Building on Executive Order 13,636 to Encourage Information Sharing for Cybersecurity Purposes," *Harvard Journal of Law and Public Policy* 37, no. 2 (2014).

12. For example, see Rachel Nusbaum, "CISA Isn't about Cybersecurity, It's About Surveillance," American Civil Liberties Union, March 13, 2015, https://www.aclu.org/blog/cisa-isnt-about-cybersecurity-its-about-surveillance.

13. Indeed, the text of CISA expressly authorizes federal agencies to analyze data collected as part of a cyberthreat indicator for terrorism investigations and criminal cases. See Andrea Castillo, "What You Should Know About CISA," *Plain Text*, *Medium*, March 23, 2015, https://medium.com/plain-text/what-you-should-know-about-cisa-950c395dddf6.

14. Presidential Decision Directive No. 63, 63 Fed. Reg. 41804 (1998).

15. "Government–Private Sector Relations" (White Paper, ISAC Council, January 31, 2004), http://www.isaccouncil.org/images/Government_Private_Sector_Relations_013104.pdf.

16. Eli Dourado and Andrea Castillo, "Dozens of Federal Cybersecurity Offices Duplicate Efforts with Poor Coordination," Mercatus Center at George Mason University, April 14, 2015, http://mercatus.org/publication/dozens-federal-cybersecurity-offices-duplicate-efforts-poor-coordination.

17. Eli Dourado and Andrea Castillo, "Poor Federal Cybersecurity Reveals Weakness of Technocratic Approach," (Mercatus on Policy, Mercatus Center at George Mason University, Arlington, VA, June 2015), http://mercatus.org/publication/poor-federal-cybersecurity-reveals-weakness-technocratic-approach; Paul Rosenzweig, "Cyber Security: A Complex 'Web' of Problems" (WebMemo No. 2991, Heritage Foundation, August 26, 2010), http://www.heritage.org/research/reports/2010/08/cyber-security-a-complex-web-of-problems.

18. Government Accountability Office, *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*, GAO-13-187, 2013, http://www.gao.gov/assets/660/652170.pdf.

19. Joseph Straw, "Food Sector Abandons Its ISAC," *Security Management*, ASIS International, September 1, 2008, https://sm.asisonline.org/Pages/Food-Sector-Abandons-Its-ISAC.aspx.

20. Office of the Inspector General, Department of Homeland Security, *DHS' Efforts to Coordinate the Activities of Federal Cyber Operations Centers*, OIG-14-02, October 24, 2013, https://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-02_Oct13.pdf.

21. Government Accountability Office, *Information Security: Agencies Need to Improve Cyber Incident Response Practices*, GAO-14-354, April 2014, http://www.gao.gov/assets/670/662901.pdf.

22. Senate Committee on Homeland Security and Governmental Affairs, *A Review of the Department of Homeland Security's Missions and Performance*, January 2015, http://www.hsgac.senate.gov/media/minority-media/final-coburn-oversight-report-finds-major-problems-in-dhs.

23. US Computer Emergency Readiness Team, "Alert TA14-069A, Microsoft Ending Support for Windows XP and Office 2003," March 10, 2014, https://www.us-cert.gov/ncas/alerts/TA14-069A-0, accessed December 29, 2014.

24. Phyllis Schneck, "Strengthening Public-Private Partnerships to Reduce Cyber Risks to Our Nation's Critical Infrastructure" (Testimony of before the Senate Committee on Homeland Security and Governmental Affairs and Post-Hearing Questions for the Record Submitted to Phyllis Schneck, March 26, 2014).

25. N. Eric Weiss, "Legislation to Facilitate Cybersecurity Information Sharing."

26. EINSTEIN 1, a voluntary intrusion-detection system for federal civilian agencies, intended to collect system data and send suspicious activity in real time to US-CERT for analysis and notice. EINSTEIN 2 added intrusion-prevention system capabilities to the original EINSTEIN program and made participation mandatory for all civilian agencies. The most recent iteration, EINSTEIN 3, will perform deep package inspection of network activity that can reveal and prevent both the transaction and content of network activity.

27. Office of the Inspector General, Department of Homeland Security, *Implementation Status of EINSTEIN 3 Accelerated*, OIG-14-52, March 24, 2014, https://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-52_Mar14.pdf.

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

29. Steven M. Bellovin, Scott O. Bradner, Whitfield Diffie, Susan Landau, and Jennifer Rexford, "Can It Really Work? Problems with Extending EINSTEIN 3 to Critical Infrastructure," *Harvard National Security Journal* 3, no. 1 (2012), http://harvardnsj.org/wp-content/uploads/2012/01/Vol.-3_Bellovin_Bradner_Diffie_Landau_Rexford.pdf.

30. Dourado and Castillo, "Poor Federal Cybersecurity Reveals Weakness of Technocratic Approach."

31. Office of Management and Budget, *Annual Report to Congress: Federal Information Security Management Act* (Washington, DC, Febraury 2015), http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy14_fisma_report_02_27_2015.pdf

32. Eli Dourado and Andrea Castillo, "Agencies Fail 2014 Cyber Report Card and Report Record Number of IT Breaches," Mercatus Center at George Mason University, April 29, 2015, http://mercatus.org/publication/agencies-fail-2014-cyber-report-card-and-report-record-number-it-breaches-FISMA.

33. Perera and Marks, "Newly Disclosed Hack Got 'Crown Jewels.'"

34. Zetter and Greenberg, "Why the OPM Breach Is Such a Security and Privacy Debacle."

35. Ibid.

36. David Perera, "Office of Personnel Management Didn't Encrypt Feds' Data Hacked by Chinese," *Politico*, June 4, 2015, http://www.politico.com/story/2015/06/personal-data-of-4-million-federal-employees-hacked-118655.html.

37. Damian Paletta and Siobhan Hughes, "US Agencies Join Probe of Personnel Records Theft," *Wall Street Journal,* June 10, 2015, http://www.wsj.com/articles/u-s-spy-agencies-join-probe-of-personnel-records-theft-1433936969.

38. Ibid.

39. Michael Holden, "Briton Arrested over Hack into US Department of Defense," *Reuters*, March 6, 2015, http://www.reuters.com/article/2015/03/06/us-britain-usa-hacker-idUSKBN0M214K20150306; Ellen Nakashima, "DHS Contractor Suffers Major Computer Breach, Officials Say," *Washington Post*, August 6, 2014, http://www.washingtonpost.com/world/national-security/dhs-contractor-suffers-major-computer-breach-officials-say/2014/08/06/8ed131b4-1d89-11e4-ae54-0cfe1f974f8a_story.html; Ed O'Keefe, "How Was the Justice Department Web Site Attacked?," *Washington Post*, January 20, 2012, http://www.washingtonpost.com/blogs/federal-eye/post/how-was-the-justice-department-web-site-attacked/2012/01/19/gIQA6EGHDQ_blog.html.

40. Sara Sorcher, "Obama's Info-Sharing Plan Won't Significantly Reduce Security Breaches," *Passcode, Christian Science Monitor*, March 2015, http://passcode.csmonitor.com/influencers-infosharing.

41. Robert Graham, "Whatever It Is, CISA Isn't Cybersecurity," *Errata Security*, March 18, 2015, http://blog.erratasec.com/2015/03/what-ever-it-is-cisa-isnt-cybersecurity.html.

42. "2013 Cost of Data Breach Study: Global Analysis" (Research Report, Ponemon Institute, Traverse City, MI, May 2013), http://www.ponemon.org/library/2013-cost-of-data-breach-global-analysis.

43. "Report on Cyber Security Education Project" (Research Report, Command, Control, and Interoperability Center for Advanced Data Analysis, Piscataway, NJ, June 9, 2014), http://www.ccicada.org/wp-content/uploads/2015/03/CyberSecurityEducationReport_CCICADA_6-9-14Final.pdf.

44. Many federal agencies do not require any form of strong user authentication at all. See John Fontana, "Report Says Strong Authentication Use Lagging in Federal Agencies," *ZDNet*, March 13, 2015, http://www.zdnet.com/article/report-says-strong-authentication-not-up-to-par-in-federal-agencies/.

45. "Is Your Company Ready for a Big Data Breach? The Second Annual Study on Data Breach Preparedness" (Research Report, Ponemon Institute, Traverse City, MI, September 2014), http://www.experian.com/assets/data-breach/brochures/2014-ponemon-2nd-annual-preparedness.pdf.

46. Andrea Castillo, "How CISA Threatens Both Privacy and Cybersecurity," *Reason.com*, May 10, 2015, http://reason.com/archives/2015/05/10/why-cisa-wont-improve-cybersecurity.

47. "Collaborative Security: An Approach to Tackling Internet Security Issues" (Report, Internet Society, Reston, VA, April 2015), http://www.internetsociety.org/sites/default/files/CollaborativeSecurity-v1-0.pdf.

48. Danielle Kehl, Kevin Bankston, and Andi Wilson, "Comments to the UN Special Rapporteur on Freedom of Expression and Opinion Regarding the Relationship Between Free Expression and the Use of Encryption" (Comment to the UN, New America Foundation, Washington, DC, February 10, 2015), https://static.newamerica.org/attachments/1866-oti-urges-un-human-rights-council-to-promote-the-benefits-of-strong-encryption/OTI_Crypto_Comments_UN.pdf.

49. Kim Zetter, "US Used Zero-Day Exploits Before It Had Policies for Them," *Wired*, March 30, 2015, http://www.wired.com/2015/03/us-used-zero-day-exploits-policies/.

50. Eli Dourado and Andrea Castillo, "Why the Cybersecurity Framework Will Make Us Less Secure" (Mercatus Research, Mercatus Center at George Mason University, April 2014), http://mercatus.org/publication/why-cybersecurity-framework-will-make-us-less-secure.