MERCATUS ON POLICY

Poor Federal Cybersecurity Reveals Weakness of Technocratic Approach

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 U.S. 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.

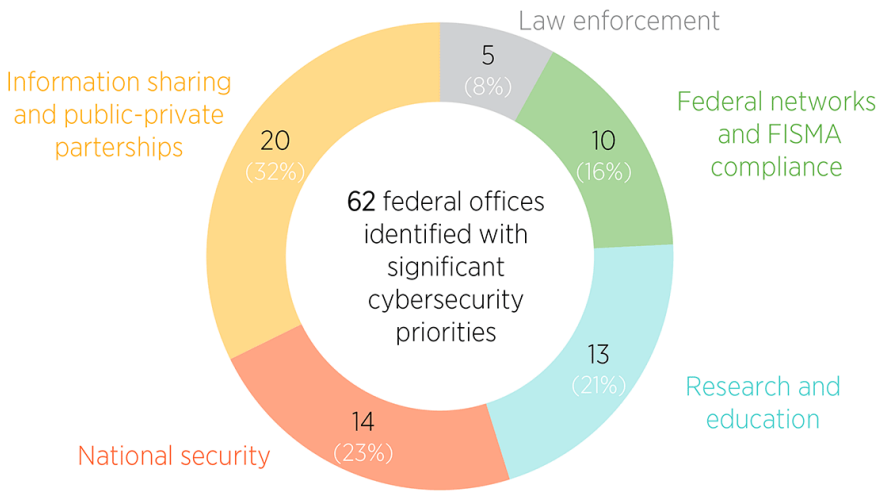
A comprehensive assessment of federal cybersecurity reveals a landscape rife with institutional uncertainty, office redundancy, and suboptimal agency outcomes. This year's catastrophic breach of the Office of Personnel Management's (OPM) unencrypted database exposing the Social Security numbers, addresses, financial information, and security clearances of over 14 million current and former federal employees, intelligence and military personnel,[1] contractors, and countless other family members, friends, and associates listed in federal background checks serves as only the latest reminder of these ongoing and dangerous vulnerabilities.[2] The typical federal response to information security vulnerabilities has been to increase spending, create new bureaucracies, or institute new rules and standards, rather than focus on results. This approach has served largely to increase the confusion of the people charged with implementing federal cybersecurity policy, to the detriment of outcomes.

This paper will review the laws and standards governing federal cybersecurity policy and will highlight how overlapping responsibilities and unclear lines of authority have accompanied increasing rates of federal information security failures. The paper will then describe how these systemic cybersecurity weaknesses demonstrate the federal government to be an especially poor candidate for managing national systems, and it will explain the shortcomings of a top-down, technocratic approach.

UNCOORDINATED BUREAUCRATIC GROWTH

The federal government has tried to coordinate effective public and private information system management through several legislative and executive means over the past two decades. President Clinton's Presidential

FIGURE 1. FEDERAL CYBERSECURITY CENTERS BY MISSION CATEGORY, 2015



Sources: Government Accountability Office, *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*, GAO-13-187, February 2013; authors' analysis of federal websites and budget documents. Note: lists of all offices and mission statements can be found in accompanying dataset: Eli Dourado, 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.

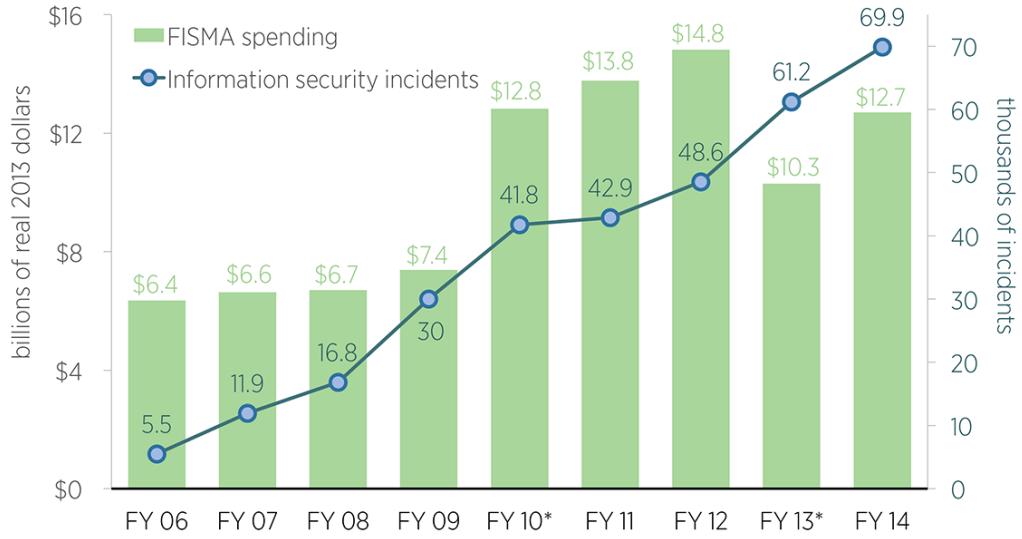
Decision Directive 63 (PDD-63) in 1998 developed an outline for a public-private partnership to "eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems."[3] Clinton's National Plan for Infrastructure Protection (NIPP) of 2000 addressed in more detail "critical infrastructure assets" deemed so vital to the nation that their incapacity would have a crippling effect on the country.[4] Congress passed the Federal Information Security Management Act (FISMA) in 2002, which outlined legislative milestones and increased federal investment in agency information security systems in an effort to meet the newly established standards by the end of the decade.[5] In 2003, President Bush implemented a new and slightly different national cybersecurity initiative called the National Strategy to Secure Cyberspace, which prioritized cybersecurity threat identification, response, and notification.[6] It did not mention PDD-63 or the NIPP once.

Five years later, Bush's classified Comprehensive National Cybersecurity Initiative (CNCI) again attempted to outline an authoritative federal cybersecurity strategy emphasizing threat detection and information sharing.[7] President Obama has likewise contributed to the thicket of federal cybersecurity, first by issuing a Cyberspace Policy Review in 2009 that encouraged a unification of overlapping policies and increased investment, education, and cyberthreat information sharing among public and private entities.[8] In 2013, Obama issued an executive order[9] calling upon the National Institute of Standards and Technology (NIST) to develop cybersecurity standards for critical infrastructure assets, called the "Cybersecurity Framework."[10] A spate of cybersecurity bills were signed into law in late 2014, which separately defined the National Cybersecurity Communications Integration Center as the main federal cyber information sharing hub,[11] authorized NIST to facilitate the Cybersecurity Framework,[12] amended the FISMA reporting processes,[13] and increased cybersecurity workforce examinations and placements.[14] Now, Congress[15] and the White House[16] have developed proposals to increase federal influence over private cybersecurity practices by extending legal liability to private corporations that share sensitive customer data with federal agencies. Yet the existing problems plaguing federal network security are substantial, unaddressed, and likely to undermine the effectiveness of these proposals.

FEDERAL CYBERSECURITY POLICY LACKS FOCUS

In spite of, or perhaps because of, these accumulating efforts and offices, federal cybersecurity policy has lacked a unified focus for as long as it has existed. The growing mass of information security procedures and

FIGURE 2. FEDERAL CYBERSECURITY SPENDING AND TOTAL REPORTED FEDERAL INFORMATION SECURITY INCIDENTS



Data Note: *OMB calculation methodologies of total FISMA spending changes in indicated years. Source: Congressional Research Service, "Cybersecurity Issues and Challenges: In Brief," December 16, 2014; Government Accountability Office, *Information Security: Federal Agencies Need to Enhance Responses to Data Breaches*, GAO-14-487T, April 2, 2014. Produced by Eli Dourado, Andrea Castillo, and Rizqi Rachmat, Mercatus Center at George Mason University, March 2015.

rules already "vary in terms of priorities and structure" while at the same time do not "specify how they link to or supersede other documents," nor "describe how they fit into an overarching national cybersecurity strategy," reports the Government Accountability Office (GAO).[17] Priorities and responsibilities change in tandem with evolving technology and security concerns. However, the complexity and inconsistency of federal cybersecurity initiatives is such that implementation has tended to diverge from the intended strategy.[18] Additionally, basic goal metrics like milestone and performance measures, cost projections, and specific roles and responsibilities for each agency are rarely considered in strategy documents.[19] Confused or overwhelmed personnel have struggled to comply with new iterations of federal cybersecurity policies, as annual FISMA reports demonstrate.[20] GAO investigations of federal incident report procedures find that agencies do not effectively or consistently follow procedures in roughly 65 percent of reported incidents.[21]

Similarly, the federal government lacks public resources detailing the total number of federal cybersecurity offices. An initial investigation finds a total of 62 separate federal cybersecurity centers as of fiscal year (FY) 2015.[22] Of these, 20 prioritized facilitating information sharing among federal offices or between public and private entities; 14 were housed by the Department of Defense (DOD) and specifically focused on "cyberwar" training, preparedness, and missions; 13 were dedicated to education and research programs; ten were tasked with maintaining federal network security or overseeing FISMA; and the remaining 5 offices were dedicated to fighting cybercrime under the direction of the Federal Bureau of Investigation (FBI).

Many of the offices were identified to operate under nearly identical mission statements with no clear distinction in operations. The GAO has reported for years that such overlapping and unclear responsibilities in federal cybersecurity policy have limited the offices' ultimate effectiveness.[23] Often, various agency representatives interpreted their responsibilities in a different way than outlined in the text of a law.[24] Merely imposing new policies on top of old ones, therefore, is unlikely to rectify the systemic barriers to security compliance that have bedeviled personnel for so many years.[25]

Additionally, the National Security Agency (NSA) assumes a larger role in federal cybersecurity than is often publicly acknowledged.[26] The NSA's intelligence culture and byzantine organization adds another level of confusion and complexity into federal cybersecurity policy that ultimately flummoxes coordination and undermines outcomes. Former NCSC director Rod Beckstrom said he resigned partially because the NSA's dominant influence in cybersecurity policy crowded out his office's efforts.[27] Additionally, the NSA has been unable to stem state-backed hacking despite its

considerable tools of data extraction and surveillance. In June of 2015, the *New York Times* and *ProPublica* revealed that the NSA and FBI had joined forces to track online activities of suspected state-backed cyberterrorists overseas by directly extracting data from the backbone of Internet traffic.[28] Still, the massive OPM hack of critical federal data was not identified by the NSA, but by an ordinary product sales demonstration.[29] More generally, it bodes poorly for security outcomes that a clandestine agency with a known bias toward weakening encryption standards[30] should take a leading, but hidden, role in cybersecurity provision.

CONFUSION AND NONCOMPLIANCE STYMIE EFFECTIVENESS

It is not surprising that, given the chaos of existing federal security directives, the rate of reported federal information security incidents has significantly increased over the years despite billions in increased FISMA investments. OMB's annual report on federal information security practices and incidents for FY 2014[31] revealed that the total number of reported federal information security failures had increased[32] by an astounding 1,169 percent, from 5,503 in FY 2006 to 69,851 in FY 2014.[33]

Some information security failures are the direct result of personnel noncompliance with established policies.[34] Policy violations, where federal employees fail to follow prescribed data management practices, constituted the largest bulk of reported failures last year behind the catchall "other" category and noncyber incidents involving physical media. The OPM, for example, did not even encrypt the sensitive datasets that were recently hacked.[35] On the other hand, compliance on paper with established federal procedures does not always translate to good security outcomes. The National Aeronautics and Space Administration (NASA) received high scores for FISMA compliance, yet reported the highest number of information security failures of all agencies in FY 2014.[36] This suggests that FISMA compliance alone does not ensure better security outcomes, so agencies that focus on optimizing FISMA metrics may be ignoring fundamental security vulnerabilities more in need of attention.

In many cases, agencies do not properly train employees in general preventative cybersecurity practices.[37] Several agencies reporting the lowest levels of personnel training—including the State Department, Department of Health and Human Services (HHS), and DOD—are prime targets for malicious hackers because they manage large and sensitive datasets, including personally identifiable information of personnel and civilians. Each of these agencies has suffered from major database hacks in recent years.[38]

Similar challenges plague even federal cybersecurity professionals. Communication problems between agency human resource departments and information technology managers result in poor outreach to qualified hiring candidates and ultimately an underqualified federal information security workforce.[39] Additionally, Chief Information Officers (CIOs) for federal offices report that compensation packages available for personnel lag far behind prevailing private sector incomes and prove inadequate to attract the "best and brightest" cybersecurity and information technology talent.[40] After hiring, many agencies—including HHS, DHS, the Department of Justice, and the Department of the Treasury—did not require cybersecurity professionals to undergo training or certification programs for several years.[41] The most recent IT Workforce Assessment for Cybersecurity study, a self-reported survey of federal cybersecurity professionals undertaken by the Federal CIO Council, finds that lowest average proficiencies of cybersecurity personnel are in digital forensics, threat analysis, and cyber operations—areas critical to robust cybersecurity provision.[42]

A CASE STUDY IN TECHNOCRATIC WEAKNESS

The federal government's continued failures to secure its own information networks indicate a fundamentally flawed approach to cybersecurity. Sweeping technocratic solutions are iteratively imposed every few years with little-to-no understanding or continuity with previous policies. Abstract consistencies in top-down planning break down on the human level as personnel struggle to make sense of redundancies and eventually ignore complex reporting and procedural standards. Fundamental issues of talent recruitment and personnel training go relatively unaddressed as offices struggle to keep up with the changing security checklists, which may or may not actually translate to good cybersecurity outcomes.

Merely increasing the number of resources or procedures dedicated to federal cybersecurity is unlikely

to improve a system built on fundamentally flawed assumptions and processes. Recent proposals to expand the federal government's role in private cybersecurity provision are more questionable still, given the federal government's failures to adequately protect even its own systems.[43] To truly improve cybersecurity preparedness, unsuccessful top-down technocratic measures should be replaced by self-organizing collaborative security approaches that emphasize flexibility, evolution, consensus, participation, and incrementalism.[44]

ENDNOTES

1. 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.
2. 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/.
3. Presidential Decision Directive No. 63, 63 Fed. Reg. 41804 (1998).
4. Executive Office of the President, "Defending America's Cyberspace: National Plan for Information Systems Protection: An Invitation to a Dialogue," January 2000, http://fas.org/irp/offdocs/pdd/CIP-plan.pdf.
5. Federal Information Security Management Act of 2002, Tit. III, E-Government Act of 2002, Pub. L. No. 107-296 (Tit. X), 116 Stat. 2259; Pub. L. No. 107-347 (Tit. III), 116 Stat. 2946. 44 U.S.C. Ch. 35, Subchapters II and III, codified at 40 U.S.C. §11331, 15 U.S.C. 278g-3 & 4, http://csrc.nist.gov/drivers/documents/FISMA-final.pdf.
6. President's Critical Infrastructure Protection Board, "National Strategy to Secure Cyberspace," February 2003, http://georgewbush-whitehouse.archives.gov/pcipb/.
7. John Rollins and Anna C. Henning, "Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations" (Congressional Research Service, Washington, DC, March 10, 2009), http://www.fas.org/sgp/crs/natsec/R40427.pdf.
8. Executive Office of the President, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure," May 8, 2009, https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.
9. Executive Order No. 13636, 78 Fed. Reg. 11739 (2013).
10. Eli Dourado and Andrea Castillo, "Why the Cybersecurity Framework Will Make Us Less Secure" (Mercatus Research, Mercatus Center at George Mason Univesity, Arlington, VA, April 17, 2014), http://mercatus.org/publication/why-cybersecurity-framework-will-make-us-less-secure.
11. National Cybersecurity Protection Act of 2014, Pub. L. No. 113-282, 128 Stat. 3066 (2014).
12. Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274, 128 Stat. 2971 (2014).
13. Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (2014).
14. Cybersecurity Workforce Assessment Act, Pub. L. No. 113-246, 128 Stat. 1193 (2014).
15. Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. (2015).
16. Exec. Order No. 13691, 80 Fed. Reg. 9347 (2015).
17. Government Accountability Office, *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*, GAO-13-187, February 2013, http://www.gao.gov/assets/660/652170.pdf.
18. For example, in 2013, OMB decided to transfer its cybersecurity oversight activities to the Department of Homeland Security (DHS) despite the fact that FISMA clearly delegated this to OMB. Ibid.
19. Ibid.
20. Office of Management and Budget, *Annual Report to Congress: Federal Information Security Management Act*, 2015, http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy14_fisma_report_02_27_2015.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. This analysis is preliminary. Some federal offices tasked with primary cybersecurity duties may not have come up in the first investigation, and offices that were counted could be categorized in more than one category. See: 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.
23. Government Accountability Office, *Cybersecurity: National Strategy, Roles, and Responsibilities*.
24. For example, in 2013, OMB decided to transfer its cybersecurity oversight activities to DHS despite the fact that FISMA clearly delegated this to OMB. New executive orders and legislative additions to cybersecurity policy may very likely be interpreted by agencies in a different way than intended.
25. For a discussion of the broader problem of regulatory accumulation, see: Patrick McLaughlin and Richard Williams, "The Consequences of Regulatory Accumulation and a Proposed Solution" (Mercatus Working Paper, Mercatus Center at George Mason University, Arlington, VA, February 2014), http://mercatus.org/publication/consequences-regulatory-accumulation-and-proposed-solution.
26. Susan Landau, "Under the Radar: NSA's Efforts to Secure Private-Sector Telecommunications Infrastructure," *Journal of National Security Law and Policy* 7, no. 3 (2015): 411–442.
27. Rod Beckstrom, Letter of Resignation to Department of Homeland Security Director Janet Napolitano, March 5, 2009, http://online.wsj.com/public/resources/documents/BeckstromResignation.pdf.
28. Charlie Savage, Julia Angwin, Jeff Larson, and Henrik Moltke,

"Hunting for Hackers, NSA Secretly Expands Internet Spying at US Border," *New York Times*, June 4, 2015, http://www.nytimes.com/2015/06/05/us/hunting-for-hackers-nsa-secretly-expands-internet-spying-at-us-border.html.

29. 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.

30. Jacob Aron and Paul Marks, "How NSA Weakens Encryption to Access Internet Traffic," *New Scientist*, September 6, 2013, http://www.newscientist.com/article/dn24165-how-nsa-weakens-encryption-to-access-internet-traffic.html.

31. Office of Management and Budget, *Annual Report to Congress: Federal Information Security Management Act*.

32. Part of the rise in reported information security incidents in FY 2014 can be attributed to "enhanced capabilities to identify, detect, manage, recover and respond to these incidents"—through enhanced incident reporting requirements to US-CERT and the new EINSTEIN 3 threat detection and repulsion software of the DHS's National Cybersecurity Protection System—as well as an overall increase in actual incidents. Accordingly, the true number of federal information security incidents in previous years may have been even greater than initially reported. Ibid.

33. 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.

34. Office of Management and Budget, *Annual Report to Congress: Federal Information Security Management Act.*

35. 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.

36. Andrea Castillo, "Feds Fail 2014 Cyber Report Card," *Plain Text*, *Medium*, March 19, 2015, https://medium.com/plain-text/feds-fail-2014-cyber-report-card-d5d3f233afcd.

37. Office of Management and Budget, *Annual Report to Congress: Federal Information Security Management Act*.

38. Evan Perez and Shimon Prolupecz, "Sources: State Dept. Hack the 'Worst Ever,'" *CNN*, March 10, 2015, http://www.cnn.com/2015/03/10/politics/state-department-hack-worst-ever; Andrea Peterson and Jason Millman, "HealthCare.gov Server Hacked. But HHS Says No Consumer Information Taken," *Washington Post*, September 4, 2014, http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/04/healthcare-gov-server-hacked-but-hhs-says-no-consumer-information-taken; 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.

39. Partnership for Public Service and Booz Allen Hamilton, *Cyber In-Security: Strengthening the Federal Cybersecurity Workforce,* July 2009, http://ourpublicservice.org/publications/viewcontentdetails.php?id=121.

40. Ibid.

41. Government Accountability Office, *Cybersecurity Human Capital: Initiatives Need Better Planning and Coordination*, GAO-12-8, 2011, http://www.gao.gov/products/GAO-12-8.

42. Department of Homeland Security and Chief Information Officer's Council, *2012 Information Technology Workforce Assessment for Cybersecurity (ITWAC) Summary Report*, March 2013, https://cio.gov/wp-content/uploads/downloads/2013/04/ITWAC-Summary-Report_04-01-2013.pdf.

43. Andrea Castillo and Eli Dourado, "'Information Sharing': No Panacea for American Cybersecurity Challenges" (Mercatus on Policy, Mercatus Center at George Mason University, Arlington, VA, June 2015).

44. "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.