The Heritage Foundation
LEADERSHIP FOR AMERICA

BACKGROUNDER

No. 2695 | MAY 24, 2012

The Alarming Trend of Cybersecurity Breaches and Failures in the U.S. Government

Paul Rosenzweig

Abstract
The number of cybersecurity attacks on, and breaches within, the United States government has been growing. The U.S. Senate is now gearing up to debate cybersecurity legislation—and will have to vote on whether the federal government should regulate cybersecurity measures of the private sector as well as those of government. The government's track record on cybersecurity does not inspire confidence that it can devise effective cybersecurity regulations for the private sector. Cybersecurity for the nation should be a cooperative effort between the private sector and the government, with each contributing in its own way. Onerous regulations are not the solution to the ever-expanding reality of cyberthreats.

This paper, in its entirety, can be found at **http://report.heritage.org/bg2695**

Produced by the Douglas and Sarah Allison Center for Foreign Policy Studies

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

As the Senate prepares for its debate over cybersecurity legislation, one of the most important questions it will have to address is whether the federal government, acting through the Department of Homeland Security (DHS), should play a significant role in crafting cybersecurity regulations that will govern activities of the private sector as well as of government. Proponents of such a role, embodied in Title I of the Lieberman–Collins Cybersecurity Act of 2012, contend that the private sector has done an inadequate job of protecting itself and that market incentives have not developed appropriately to promote self-protection. Opponents of Title I argue that the government is ill equipped to develop effective cybersecurity regulations and that the regulatory process is too cumbersome for the development of rules and standards applicable to the dynamic cyberdomain.

One possible approach to resolving this dispute is to ask whether the federal government has done an effective job of protecting its own networks and cyberdata. To the extent that it has, it might be deemed an appropriate source of private-sector standards; to the extent it has not, a contrary opinion

Talking Points

- As the Senate prepares for its debate on cybersecurity legislation, one of the most important questions it must address is whether the federal government should play a significant role in crafting cybersecurity regulations that will govern the private sector as well as government.
- Proponents of government regulation contend that the private sector has not protected itself adequately, and that market incentives have not worked. Opponents argue that the regulatory process is too cumbersome for the development of rules and standards applicable to the dynamic cyberdomain.
- The federal government's record on cybersecurity—a growing list of breaches, failures, and oversights—does not inspire confidence that it can provide a solution to the cybersecurity threats faced by the private sector.
- Cybersecurity should be a cooperative effort between the private sector and the government, with each contributing in its own way.

might be formed. It is, thus, worth considering the extent of cyber-attacks on, and breaches within, the federal government since 2004.[1] To be sure, the significance of certain attacks and breaches lies in the eye of the beholder—the compiler of any list necessarily exercises judgment in making the determination. And, without a doubt, a comparable list of significant attacks on, and breaches within, the private sector would be far more extensive. Nevertheless, the substantial number of significant, successful attacks on federal systems should play a role in determining whether to entrust DHS with a regulatory role in the private-sector cyberdomain. The list is alphabetical by agency.[2]

Central Intelligence Agency

1. CIA Official Website—June 2011. The CIA's homepage was shut down by a cyber-attack by LulzSec, an anonymous hacker group believed to hack websites simply for fun.[3]

U.S. Congress

2. Senate—June 2011. The Sergeant at Arms confirmed that the Senate website had been hacked after files from the website were posted online, indicating that Lulz Sec had broken into the Senate's computer network.[4]

3. Office of Senator Bill Nelson (D–FL)—March 2009. Senator Nelson confirmed that his personal office computers had been subject to three separate attacks by China-based hackers.[5]

4. Offices of Representative Frank Wolf (R–VA) and the House Foreign Affairs Committee—August 2006. Representative Wolf announced that the computers at his personal office, a number of unnamed Representatives' offices, and the office of the House Foreign Affairs Committee had been hacked by China-based hackers.[6]

U.S. Department of Agriculture

5. Washington, D.C., Headquarters—June 2006. The Department of Agriculture was subject to a cyber-attack by an unknown entity, during which the names, Social Security numbers, and photographs of 26,000 employees were stolen.[7]

U.S. Department of Commerce

6. Economic Development Administration—February 2012. The Department of Commerce had to disconnect its computers from the Internet because unknown intruders injected a virus into the Economic Development Administration's computer network.[8]

1. The first version of this list was published on *Lawfare*: Paul Rosenzweig, "Significant Cyber Attacks on Federal Systems—2004–Present," *Lawfare*, May 7, 2012, http://www.lawfareblog.com/2012/05/significant-cyber-attacks-on-federal-systems-2004-present/ (accessed May 15, 2012). The list was not originally compiled by the author but has been vetted by him.
2. Most of the incidents listed involve breaches of cybersecurity in the network. Some real-world events, such as the theft of a hard drive or loss of a disk, are deemed cyber-related because the data medium being used is cyber-based. In some ways, such a theft is no different than the theft of a car—but the use of a cyber medium greatly magnifies the scope of the damage and loss, turning a difference in degree into a difference in kind. While the theft of a car results in the loss of a single car, the theft or loss of a hard drive compromises thousands, if not hundreds of thousands, of people. Today's data-storage media both enable the ease of the crime and exacerbate the damage.
3. Marc Chacksfield, "CIA Website and FBI Hacked by LulzSec," Techradar, June 16, 2011, http://www.techradar.com/news/internet/cia-website-and-fbi-hacked-by-lulzsec-966715 (accessed May 9, 2012).
4. Diane Bartz and Thomas Ferraro, "Hackers Break into Senate Computers," Reuters, June 13, 2011, http://www.reuters.com/article/2011/06/13/us-cybersecurity-usa-senate-idUSTRE75C5JI20110613 (accessed May 9, 2012).
5. Josh Rogin, "Hackers Based in China Break Into Florida Senator's Office Computers," Young Professionals in Foreign Policy, March 24, 2009, http://www.ypfp.org/content/hackers-based-china-break-florida-senator%E2%80%99s-office-computers (accessed May 9, 2012).
6. News release, "Wolf Reveals House Computers Compromised by Outside Source," Frank Wolf, 10th District of Virginia, June 11, 2008, http://wolf.house.gov/index.cfm?sectionid=34&parentid=6&sectiontree=6,34&itemid=1174 (accessed May 8, 2012).
7. "Cyber Attacks Continue to Grow," MSNBC, May 29, 2009, http://www.msnbc.msn.com/id/31000126/ns/technology_and_science-security/t/cyber-attacks-continue-grow/ (accessed May 8, 2012).
8. Lisa Rein, "For Commerce Unit Hit by Computer Virus, Hardship of Being Unplugged Has Upside," *The Washington Post*, April 9, 2012, http://www.washingtonpost.com/politics/for-agency-a-loss-of-technology-has-had-down--and-upsides/2012/04/08/gIQAvpAY5S_story.html (accessed May 8, 2012).

7. Commerce Department Website—December 2009. The Commerce Department accidentally posted personally identifiable information and Social Security numbers on its website, and did not notify employees until seven weeks after the fact.[9]

8. Secretary of Commerce—December 2007. Spying software was found on the electronic devices of the Commerce Secretary following a trip to China with the Joint Commission on Commerce and Trade.[10]

9. Bureau of Industry and Security—October 2006. The Department of Commerce had to take the Bureau of Industry and Security's networks offline for several months and replace hundreds of computers because its networks were hacked by unknown foreign intruders. The bureau reviews confidential information on high-tech exports.[11]

U.S. Department of Defense (DOD)

10. F-35 Fighter-Plane Development—February 2012. The Commerce Department's Bureau of Industry and Security announced that delays and high costs for the development of the F-35 stemmed from addressing cybersecurity after China-based hackers stole classified information discussing the technology.[12]

11. Unmanned Aerial Vehicle, Afghanistan—December 2011. An RQ-170 stealth drone went missing and apparently crashed near the Iranian border. Iran claimed to have downed the drone through a cyber-attack.[13]

12. Defense Department Contractor—July 2011. In a speech unveiling the Defense Department's cyberstrategy, the Deputy Secretary of Defense mentioned that a defense contractor's computer was hacked, and 24,000 files relating to sensitive systems being developed were stolen by unidentified hackers.[14]

13. National Guard—December 2010. A computer containing the personal information on 650 soldiers was stolen from Santa Fe, New Mexico, headquarters by an unknown entity.[15]

14. The Army—April 2010. The Army lost personal data of reservists through unknown means and has warned affected reservists to "check credit bureau reports and be aware of the possibilities of identity theft."[16]

15. Unmanned Aerial Vehicle (UAV) Feeds—December 2009. Downlinks from U.S. UAVs were hacked by Iraqi insurgents using inexpensive file-sharing software, allowing them to see what the UAVs had viewed.[17]

16. U.S. Central Command—November 2008. Classified networks at the Defense Department and Central Command relating to U.S. involvement in Iraq and Afghanistan were subject to a cyber-attack thought to have originated in Russia.[18]

17. Secretary of Defense's E-Mail Account—June 2007. The Secretary of Defense's unclassified

9. Joe Davidson, "Commerce Dept. Slow to Notify Employees of Security Breach," *The Washington Post*, January 27, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/01/26/AR2010012603509.html?hpid=news-col-blog (accessed May 9, 2012).
10. Shane Harris, "China's Cyber-Militia," *National Journal*, May 31, 2008, http://www.nationaljournal.com/magazine/china-s-cyber-militia-20080531 (accessed May 9, 2012).
11. Gregg Keizer, "Chinese Hackers Hit Commerce Department," *Information Week*, October 6, 2006, http://www.informationweek.com/news/193105227 (accessed May 8, 2012).
12. "Did Chinese Espionage Lead to F-35 Delays?" Defense Tech, February 6, 2012, http://defensetech.org/2012/02/06/did-chinese-espionage-lead-to-f-35-delays/ (accessed May 8, 2012).
13. Greg Jaffe and Thomas Erdbrink, "Iran Says It Downed U.S. Stealth Drone; Pentagon Acknowledges Aircraft Downing," *The Washington Post*, December 4, 2011, http://www.washingtonpost.com/world/national-security/iran-says-it-downed-us-stealth-drone-pentagon-acknowledges-aircraft-downing/2011/12/04/gIQAyxa8TO_story.html (accessed May 9, 2012).
14. David Perera, "24,000 Files Stolen from DoD Contractor in Single March Attack," Fierce Homeland Security, July 17, 2011, http://www.fiercehomelandsecurity.com/story/24000-files-stolen-dod-contractor-single-march-attack/2011-07-17 (accessed May 9, 2012).
15. Celina Westervelt, "Soldiers' Personal Information Stolen," KRQE News, January 13, 2011, http://www.krqe.com/dpp/news/local/southeast/soldiers'-personal-information-stolen- (accessed May 8, 2012).
16. Martin Evans, "Army Warns Reservists of Identity Theft Threat," *Newsday*, April 22 2010, http://www.newsday.com/news/new-york/army-warns-reservists-of-identity-theft-threat-1.1876244 (accessed May 8, 2012).
17. Siobhan Gorman, Yochi J. Dreazen, and August Cole, "Insurgents Hack U.S. Drones," *The Wall Street Journal*, December 17, 2009, http://online.wsj.com/article/SB126102247889095011.html (accessed May 8, 2012).
18. Julian E. Barnes, "Pentagon Computer Networks Attacked," *Los Angeles Times*, November 28, 2008, http://articles.latimes.com/2008/nov/28/nation/na-cyberattack28 (accessed May 8, 2012).

e-mail account was hacked by unknown foreign intruders.[19]

18. National Defense University—May 2007. Spyware on the university's computer system left the university's e-mail vulnerable to attacks; the university ultimately had to take its systems offline due to intrusions by unknown foreign hackers.[20]

19. Naval War College—November 2006. The Naval War College in Rhode Island had to shut down its computer systems for two weeks following a cyber-attack. The Naval War College develops strategies for naval warfare, as well as for cybersecurity and cyberwarfare.[21]

20. Non-Classified Internet Provider Router Network—August 2006. A senior Air Force officer announced that "China has downloaded 10 to 20 terabytes of data from the NIPRNet."[22]

U.S. Department of Education

21. Computer Theft—August 2006. Computers containing personal information of grant reviewers were stolen by unknown thieves.[23]

U.S. Department of Energy (DOE)

22. National Nuclear Security Administration (NNSA)—October 2011. A report issued by the Energy Department disclosed that the NNSA had been hit by recent successful cyber-attacks perpetrated by unknown attackers.[24]

23. Pacific Northwest National Laboratory (PNNL)—July 2011. PNNL shut down access to its networks after learning it was subject to a highly sophisticated cyber-attack by an unknown entity.[25]

24. Thomas Jefferson National Accelerator Facility (TJNAF)—July 2011. Thomas Jefferson National Laboratory shut down access to its networks after learning it was subject to a highly sophisticated cyber-attack by an unknown entity.[26]

25. Oak Ridge National Laboratory (ORNL)—April 2011. ORNL, home to powerful supercomputers, shut down access to the Internet after employees received e-mails with a link that allowed the unknown attackers to siphon off data. ORNL reported that a "few megabytes" of data were stolen.[27]

26. Oak Ridge National Laboratory—October 2007. Over a thousand staffers at ORNL received an e-mail with an attachment that, when opened, provided unknown intruders with access to the lab's databases.[28]

U.S. Department of Homeland Security (DHS)

27. DHS Website—February 2012. The DHS website was taken down due to a cyber-attack, attributed to the hacker group Anonymous.[29]

28. Homeland Security Information Network (HSIN)—May 2009. HSIN was hacked by unknown intruders, who gained access to state and federal information. The HSIN is intended to be a

19. "Significant Cyber Incidents Since 2006," Center for Strategic and International Studies, May 4, 2012, http://csis.org/files/publication/120504_Significant_Cyber_Incidents_Since_2006.pdf (accessed May 8, 2012).
20. Ibid.
21. Josh Rogin, "China Is Suspected of Hacking into Navy site," *Federal Computer Week*, December 4, 2006, http://fcw.com/articles/2006/12/04/china-is-suspected-of-hacking-into-navy-site.aspx?sc_lang=en (accessed May 9, 2012).
22. Dawn S. Onley and Patience Wait, "Red Storm Rising," *Government Computer News*, August 7, 2006, http://gcn.com/articles/2006/08/17/red-storm-rising.aspx (accessed May 9, 2012).
23. Identity Theft Resource Center, "2006 Breach List," April 1, 2009, http://www.idtheftcenter.org/artman2/uploads/1/ITRC_Breach_Report_20061231.pdf (accessed May 9, 2012).
24. "Energy Department Discloses Cyber Attacks," Reuters, October 24, 2011, http://www.foxbusiness.com/technology/2011/10/24/energy-department-discloses-cyber-attacks/ (accessed May 8, 2012).
25. "Government Facilities Targets of Cyber Attacks," Reuters, July 6, 2011, http://ca.reuters.com/article/technologyNews/idCATRE7656M020110706 (accessed May 8, 2012).
26. Ibid.
27. Kim Zetter, "Top Federal Lab Hacked in Spear-Phishing Attack," *Wired*, April 20, 2011, http://www.wired.com/threatlevel/2011/04/oak-ridge-lab-hack/ (accessed May 9, 2012).
28. "Significant Cyber Incidents Since 2006," Center for Strategic and International Studies.
29. "Department of Homeland Security Website Hacked by Anonymous," *Russia Today*, March 7, 2012, http://rt.com/usa/news/homeland-security-website-anonymous-473/ (accessed May 8, 2012).

secure portal for information sharing among federal, state, and industry partners.[30]

29. DHS Washington, D.C., Headquarters—September 2007. Dozens of DHS computers and servers were hacked—the cyber break-ins were traced to a Chinese-language website, through which an unknown amount of sensitive information was stolen. The contractor hired to protect DHS computers tried to hide the incident from DHS, citing the fact that DHS had stopped paying for security monitoring services.[31]

30. DHS Washington, D.C., Headquarters—June 2007. DHS officials acknowledged that two internal DHS servers were infected with computer malware designed to steal passwords and other sensitive data.[32]

31. DHS Washington, D.C., Headquarters—2005–2006. A 2007 report by the Government Accountability Office cited 884 cyber-attacks on DHS during 2005 and 2006.[33]

U.S. Department of the Interior (DOI)

32. National Business Center, Denver, CO—May 2010. The center reported that it had lost a computer disk containing the personal information of 7,500 employees.

33. DOI Audit—November 2009. The DOI failed a cybersecurity audit conducted by the DOI Inspector General, which stated that the agency falls short of security requirements.[34]

34. DOI Washington, D.C., Headquarters—February 2002. The DOI was forced, under court order, to disconnect all computers from the Internet until it could prove that it had fixed major security problems, which turned out to take two months.[35]

U.S. Department of Justice (DOJ)

35. DOJ Websites—January 2012. The hacker group Anonymous claimed responsibility for taking down the DOJ websites usdoj.gov and justice.gov in a cyber-attack to protest the FBI shutting down Megaupload.com, one of the largest file-sharing websites in the world.[36]

Federal Bureau of Investigation (FBI)

36. FBI–Scotland Yard Conference Call Discussing the Hacker Group Anonymous—February 2012. Members of Anonymous intercepted and posted a recording of the conference call online.[37]

37. FBI Website—January 2012. Anonymous claimed credit for taking down the FBI website, FBI.gov, in a cyber-attack to protest the FBI shutting down Megaupload.com.[38]

38. FBI Phone Network—June 2011. The FBI's phone network was taken down due to a cyber-attack by LulzSec.[39]

U.S. Department of State

39. Bureau of East Asian and Pacific Affairs—June 2006. The State Department confirmed that

30. Ben Bain, "Information-Sharing Platform Hacked," *Federal Computer Week*, May 13, 2009, http://fcw.com/Articles/2009/05/13/Web-DHS-HSIN-intrusion-hack.aspx (accessed May 9, 2012).
31. Ellen Nakashima and Brian Krebs, "Contractor Blamed in DHS Data Breaches," *The Washington Post*, September 24, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/09/23/AR2007092301471_pf.html (accessed May 9, 2012).
32. Robert Westervelt, "DHS Suffered More than 800 Cyber Attacks in Two Years," *Computer Weekly*, June 25, 2007, http://www.computerweekly.com/news/2240081110/DHS-suffered-more-than-800-cyber-attacks-in-two-years (accessed May 8, 2012).
33. Ibid.
34. J. Nicholas Hoover, "Department of Interior Fails Cybersecurity Audit," *Information Week*, November 10, 2009, http://www.informationweek.com/news/government/security/221601054 (accessed May 8, 2012).
35. "Net (Still) Out at Department of Interior," CNN, February 6, 2002, http://articles.cnn.com/2002-02-06/tech/doi.security.idg_1_trust-funds-internet-access-security-problems?_s=PM:TECH (accessed May 9, 2012).
36. "Department of Justice Site Hacked after Megaupload Shutdown, Anonymous Claims Credit," *The Washington Post*, January 20, 2012, http://www.washingtonpost.com/business/economy/department-of-justice-site-hacked-after-megaupload-shutdown-anonymous-claims-credit/2012/01/20/gIQAl5MNEQ_story.html (accessed May 9, 2012).
37. Scott Shane, "F.B.I. Admits Hacker Group's Eavesdropping," *The New York Times*, February 3, 2012, https://www.nytimes.com/2012/02/04/us/fbi-admits-hacker-groups-eavesdropping.html?_r=1 (accessed May 9, 2012).
38. Matt Peckham, "10 Sites Skewered by Anonymous, Including FBI, DOJ, U.S. Copyright Office," *Time*, January 20, 2012, http://techland.time.com/2012/01/20/10-sites-skewered-by-anonymous-including-fbi-doj-u-s-copyright-office/ (accessed May 9, 2012).
39. Marc Chacksfield, "CIA Website and FBI Hacked by LulzSec," Techradar, June 16, 2011, http://www.techradar.com/news/internet/cia-website-and-fbi-hacked-by-lulzsec-966715 (accessed May 9, 2012).

its networks at its headquarters and offices dealing with Asia were subject to an attack that began at U.S. embassies in the East Asia–Pacific region. Unknown foreign intruders downloaded sensitive information and passwords.[40]

40. Washington, D.C., Headquarters—2005–2008. A State Department employee illegally accessed a State Department database that contained more than 60 passport application files.[41]

U.S. Department of Transportation (DOT)

41. National Highway Traffic Safety Administration (NHTSA)—June 2010. Canadian bloggers discovered that the NHTSA was inadvertently posting sensitive personal information on its website.[42]

42. DOT Website—July 2009. The DOT website was shut down by a cyber-attack perpetrated by unknown hackers that was part of a larger effort to shut down websites in the United States and South Korea.[43]

Federal Aviation Administration (FAA)

43. FAA Computer Networks—May 2009. A report released by the Department of Transportation acknowledged that the FAA administrative networks that manage air-traffic flow and electric power were subject to cyber-attacks by unknown hackers who gained access to data used to manage the network.[44]

U.S. Department of the Treasury

44. Treasury Department Website—July 2009. The Treasury website was shut down by the same cyber-attack that affected the DOT the same month, which was part of a larger effort to bring down websites in the United States and South Korea.[45]

U.S. Department of Veterans Affairs (VA)

45. VA Employee Robbed—May 2009. Thieves stole electronic records, containing information on 26.5 million people, from the residence of a VA employee who had not been authorized to take the electronic equipment home.[46]

Federal Trade Commission (FTC)

46. FTC Online-Security Website—January 2012. The website run by the FTC dedicated to cybersecurity education, OnGuardOnline.gov, was taken down and defaced by a cyber-attack perpetrated by a hacker group known as AntiSec.[47]

47. FTC Main Website—July 2009. The FTC website was shut down by a cyber-attack that was part of a larger effort to bring down websites in the United States and South Korea.[48]

National Aeronautics and Space Administration (NASA)

48. Various NASA Servers—2010–2011. NASA was subject to 5,400 security incidents in 2010 and 2011, during which

40. "Computer Hackers Attack State Dept.," *The New York Times*, July 12, 2006, http://www.nytimes.com/2006/07/12/washington/12hacker.html (accessed May 9, 2011), and Larry Greenemeier, "State Department Releases Details of Computer System Attacks," *Information Week*, July 13, 2006, http://www.informationweek.com/news/190303153 (accessed May 9, 2012).
41. News release, "State Department Employee Sentenced for Illegally Accessing Confidential Passport Files," U.S. Department of Justice, March 24, 2010, http://www.justice.gov/opa/pr/2010/March/10-crm-304.html (accessed May 8, 2012).
42. Edward Niedermeyer, "NHTSA's Complaint Database Leaks Private Information Like a Sieve," The Truth About Cars, June 3, 2010, http://www.thetruthaboutcars.com/nhtsas-complaint-database-leaks-private-information-like-a-sieve/ (accessed, May 9, 2012).
43. Martyn Williams, "Cyber Attack His [sic] South Korean Web Sites," *PC World*, July 8, 2009, http://www.pcworld.com/article/168027/cyber_attack_his_south_korean_web_sites.html (accessed May 9, 2012).
44. Siobhan Gorman, "FAA's Air-Traffic Networks Breached by Hackers," *The Wall Street Journal* May 7, 2009, http://online.wsj.com/article/SB124165272826193727.html (accessed May 10, 2012).
45. "U.S. Eyes N. Korea for 'Massive' Cyber Attacks," MSNBC, July 9, 2009, http://www.msnbc.msn.com/id/31789294/ns/technology_and_science-security/t/us-eyes-n-korea-massive-cyber-attacks/ (accessed May 9, 2012).
46. Bill Brenner, "Personal Data on 26.5 million Veterans Stolen," Search Security, May 23, 2006, http://searchsecurity.techtarget.com/news/1189759/Personal-data-on-265-million-veterans-stolen (accessed May 8, 2012).
47. John Ribeiro, "U.S. Government Online Security Website Hacked," *PC World*, January 24, 2012, http://www.pcworld.idg.com.au/article/413253/u_government_online_security_website_hacked/ (accessed May 16, 2012).
48. "U.S. Eyes N. Korea for 'Massive' Cyber Attacks," MSNBC.

unknown hackers gained "full functional control" of important systems 13 times.[49]

49. NASA Satellite—November 2011. The U.S.–China Economic and Security Review Commission announced that suspected Chinese hackers, through malicious cyber-activity, took control of two NASA satellites for more than 11 minutes over the course of 2007 and 2008.[50]

50. Jet Propulsion Laboratory—May 2011. The laboratory's website was compromised due to a cyber-attack by unknown hackers.[51]

51. Goddard Earth Observing System—May 2011. A Romanian hacker known as "Tinkode" gained access to information contained on servers for the satellite-based Earth-observation system.[52]

52. International Space Station—March 2011. A laptop containing the codes to control the International Space Station was stolen; 48 other NASA mobile computing devices were stolen or lost between April 2009 and April 2011 that contained sensitive information, including Social Security numbers.[53]

53. Jet Propulsion Laboratory—2009. The Office of the Inspector General reported that various hackers had compromised one of NASA's key mission networks, making thousands of unauthorized connections to the network and stealing export-restricted data from NASA Jet Propulsion Laboratory systems.[54]

54. NASA Washington, D.C., Headquarters—December 2006. NASA blocked all e-mails with attachments before shuttle launches for fear its network would be hacked by unknown foreign intruders.[55]

55. Various NASA Servers—2004. Suspected Chinese hackers, code-named Titan Rain by the FBI, stole a significant amount of information from sensitive networks at NASA and military labs.[56]

56. Ames Research Center—2004. A cyber-attack by an unknown hacker on the Ames Research Center forced the agency to disconnect its supercomputers from the Internet in order to limit the loss of secure data.[57]

57. X-Ray Satellite and Goddard Space Flight Center—September 1998. NASA investigators reported that the failure of an x-ray satellite was due to a cyber-attack on the Goddard Space Flight Center.[58]

National Archives and Records Administration (NARA)

58. NARA Washington, D.C., Headquarters—April 2009. A hard drive containing Social Security numbers of more than 100,000 people who had visited or worked in the White House during the Clinton Administration was lost.[59]

U.S. Office of Personnel Management (OPM)

59. USAJOBS.gov—January 2009. The Office of Personnel Management website and database for USAJOBS.gov, the federal

49. John Leyden, "NASA Lost 'Full Control' to Hackers, Pwned 13 Times Last Year," *The Register*, March 5, 2012, http://www.theregister.co.uk/2012/03/05/nasa_security_congressional_testimony/ (accessed May 8, 2012).
50. Jason Ryan, "US Satellites Compromised by Malicious Cyber Activity," ABC News, November 16, 2011, http://abcnews.go.com/blogs/politics/2011/11/us-satellites-compromised-by-malicious-cyber-activity/ (accessed May 8, 2012).
51. Robert McMillan, "NASA, Stanford Websites Hit by Search Engine Scammers," *PC World*, May 9, 2011, http://www.pcworld.com/businesscenter/article/227482/nasa_stanford_websites_hit_by_search_engine_ scammers.html (accessed May 8, 2012).
52. Paul Roberts, "Hack Targets NASA's Earth Observation System," Threat Post, May 17, 2011, http://threatpost.com/en_us/blogs/hack-targets-nasas-earth-observation-system-051711 (accessed May 9, 2012).
53. Ted Thornhill, "Stolen Nasa Laptop 'Contained the Codes to Control the International Space Station,'" *Daily Mail*, March 1, 2012, http://www.dailymail.co.uk/sciencetech/article-2108683/Stolen-Nasa-laptop-contained-codes-control-Space-Station.html (accessed May 9, 2012).
54. J. Nicholas Hoover, "NASA Servers at High Risk of Cyber Attack," *Information Week*, March 30, 2011, http://www.informationweek.com/news/government/security/229400618 (accessed May 8, 2012).
55. "Significant Cyber Incidents Since 2006," Center for Strategic and International Studies.
56. Nathan Thornburgh, "The Invasion of the Chinese Cyberspies," *Time*, August 29, 2005, http://www.time.com/time/magazine/article/0,9171,1098961,00.html (accessed May 8, 2012).
57. Keith Epstein and Ben Elgin, "Network Security Breaches Plague NASA," *Bloomberg Businessweek*, November 20, 2008, http://www.businessweek.com/print/magazine/content/08_48/b4110072404167.htm (accessed May 9, 2012).
58. Ibid.
59. Jaikumar Vijayan, "Hard Drive with Clinton-Era Data Missing from National Archives," *Computer World*, May 20, 2009, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9133340 (accessed May 8, 2012).

government's employment website, allowed unknown perpetrators to gain access to private information on the site's millions of users.[60]

U.S. Copyright Office

60. Main Website—January 2012. Hacker group Anonymous claimed credit for taking down the Copyright Office website, copyright.gov, in a cyber-attack to protest the FBI shutting down Megaupload.com.[61]

Unspecified Government Agencies

61. Six Federal Agencies—August 2011. A five-year hacker endeavor called Operation Shady RAT collected data from six unknown government agencies.[62]

62. State Department Cable—April–October 2008. A State Department cable published by WikiLeaks reported that hackers stole "50 megabytes of e-mail messages and attached documents, as well as a complete list of usernames and passwords from an unspecified [U.S. government] agency."[63]

Government-Centric Approach Is Wrong

The list above is certainly grounds to be skeptical of a cybersecurity approach that gives government regulators a significant role in developing baseline security standards. The government and the private sector both have a great deal to contribute to the country's cybersecurity, and a new, expansive regulatory burden would undermine, not enhance, public-private cooperation. Instead of adding regulations, Congress should:

- **Promote Information Sharing.** The government has a great deal of cybersecurity-threat information that could help the private sector prevent similar attacks and breaches. Many private-sector entities have cybersecurity information of their own that could help other private entities as well as the government. By implementing voluntary information sharing with adequate liability and privacy protections, cybersecurity can be improved.

- **Reject Onerous Regulations.** Though it is tempting to think that government officials can mandate cybersecurity improvements for the private sector, such efforts will likely impose massive costs on the private sector, while harming innovation as entities eschew potentially superior security for mere compliance with government regulations. Indeed, most standards that the government adopts will be rendered obsolete by constantly improving technology before they can even be implemented. Americans do not need a "Cyber SarbOx" approach to this multidimensional domain.

- **Secure Government Data.** Congress and the Administration should strengthen government's cybersecurity systems. Migrating the computer networks of certain agencies to the cloud would help the government take advantage of private-sector security innovations, while also reducing costs. Other options, such as "air gapping," unplugging critical networks from the Internet altogether, should be considered. Education efforts to stop phishing and other attacks directed at government personnel should also be expanded. Once again, improving information sharing could help improve cybersecurity across the government.

Enhancing U.S. Cybersecurity Through Cooperation

The federal government's record on cybersecurity does not inspire confidence that it can provide a solution to the cybersecurity threats face by the private sector. Cybersecurity should be a cooperative effort between the private sector and the government, with each contributing in its own way. The government is in a position to collect and share important cybersecurity threat and vulnerability information, while the private sector can innovate and share information as well.

—Paul Rosenzweig *is a Visiting Fellow in the Center for Legal & Judicial Studies and the Douglas and Sarah Allison Center for Foreign Policy Studies, a division of the Kathryn and Shelby Cullom Davis Institute for International Studies, at The Heritage Foundation.*

60. "Cyber Attacks Continue to Grow," MSNBC.
61. Peckham, "10 Sites Skewered by Anonymous, Including FBI, DOJ, U.S. Copyright Office."
62. Michael Joseph Gross, "Exclusive: Operation Shady Rat—Unprecedented Cyber-Espionage Campaign and Intellectual-Property Bonanza," *Vanity Fair*, August 2, 2011, http://www.vanityfair.com/culture/features/2011/09/operation-shady-rat-201109 (accessed May 9, 2012).
63. "Significant Cyber Incidents Since 2006," Center for Strategic and International Studies.