The Heritage Foundation

ISSUE BRIEF

No. 4288 | OCTOBER 27, 2014

Continuing Federal Cyber Breaches Warn Against Cybersecurity Regulation

David Inserra and Paul Rosenzweig

Recent high-profile private-sector hacks have once again put a spotlight on the issue of cybersecurity.[1] This is a serious problem that requires legislation to improve the United States' cybersecurity posture, but the U.S. should not reflexively adopt government regulation of cyberspace as a solution. There are concerns that such a response would not be cost-effective and would have an adverse effect on innovation. It could also potentially create a mindset of compliance rather than of security. Additionally, the government's own cybersecurity track record raises questions about the effectiveness of government cyber regulations.

The following is a list of federal government cybersecurity breaches and failures, most of which occurred during 2013 and 2014. This list is part of a continuing series published by Heritage that serves as a long-term compilation of open-source data about federal cybersecurity breaches dating back to 2004.[2]

This list is in no way complete: Some hacks might not be reported or are classified, and others have yet to be realized. In September 2014, Robert Anderson, executive assistant director of the Criminal, Cyber, Response, and Services Branch of the FBI told the Senate Homeland Security Committee that if a federal department believes it hasn't been hacked, it is likely that they are simply unaware of the hack. When Senator Coburn asked for a list of all the government hacks the panelists were aware of, he acknowledged that they may have to be discussed in a closed Senate hearing.[3] Furthermore, the list below does not include the large number of private-sector failures. Nevertheless, the seriousness and number of known U.S. government cybersecurity failures undercut the argument for a government-led regulatory approach to cybersecurity.

U.S. Nuclear Regulatory Commission (NRC)

1. **NRC Systems, 2012–2014.** Unknown hackers, including foreign hackers, used phishing, targeted e-mails, and malware in a portable document format (pdf) file in the attacks on the NRC computers. It is unknown if any data were stolen, but no classified documents appear to have been downloaded.[4]

Fannie Mae

2. **Fannie Mae Website, August 2013–early 2014.** A former Fannie Mae information technology contractor used his credentials to hack a government website operated by Fannie Mae and disable features on the website. The damages cost the company and customers $69,638.[5]

Department of Defense (DOD)

3. **DOD Pharmacy Database, January 2011.** Two or more hackers infiltrated PharmacoEconomic Center, the prescription drug database for the DOD's pharmacy. The servers were down for a day, and the hackers offered to sell root access to the domain for $399 or batches of 1,000 records for $20.[6]

This paper, in its entirety, can be found at
http://report.heritage.org/ib4288

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

4. **U.S. Army Corps of Engineers' National Inventory of Dams Database, May 2012.** An employee of the National Oceanic and Atmospheric Administration (NOAA), Xiafen "Sherry" Chen, has been indicted for allegedly having accessed "restricted areas of a protected U.S. Government computer database and downloaded sensitive files from the National Inventory of Dams."[7]

5. **U.S. Navy Marine Corps Intranet, September 2013.** Iranian hackers breached the unclassified network used by the Department of the Navy to host websites and store non-sensitive information and communications. Many details of the attack remain classified, but hackers were able to enter the "bloodstream" of the Navy's unclassified network and conduct surveillance on the system. There is no evidence that any data were stolen, but it took about four months to fully purge the hackers from the system. One senior U.S. official told *The Wall Street Journal* that the attack "was a real big deal.... It was a significant penetration that showed a weakness in the system."[8]

6. **DOD Systems, October 2012–January 2013.** Lauri Love, a British man, and unnamed co-conspirators connected to the hacker group Anonymous infiltrated multiple Army systems by exploiting a flaw in Adobe's ColdFusion software, which had not been updated with the latest security patches.

   The targets included:

   - The Army Network Enterprise Technology Command Center where hackers gained access to the personal information of over 1,000 individuals;
   - The Army Materiel Command in which they accessed non-public data including competitive acquisition bids;
   - The Army Corps of Engineers server from which the hackers stole non-public information on natural resource management and the personal information of thousands of individuals from the Corps in Vicksburg, Mississippi;

[1] For more information, see Riley Walters, "Cyber Attacks on U.S. Companies in 2014," Heritage Foundation *Issue Brief* No. 4289, October 27, 2014, http://www.heritage.org/research/reports/2014/10/cyber-attacks-on-us-companies-in-2014.

[2] For earlier reports in this series, see Paul Rosenzweig and David Inserra, "Government Cyber Failures Reveal Weaknesses of Regulatory Approach to Cybersecurity," Heritage Foundation *Issue Brief* No. 3968, June 13, 2013, http://www.heritage.org/research/reports/2013/06/weaknesses-of-a-regulatory-approach-to-cybersecurity; Paul Rosenzweig, "The Alarming Trend of Cybersecurity Breaches and Failures in the U.S. Government Continues," Heritage Foundation *Issue Brief* No. 3772, November 13, 2012, http://www.heritage.org/research/reports/2012/11/cybersecurity-breaches-and-failures-in-the-us-government-continue; and Paul Rosenzweig, "The Alarming Trend of Cybersecurity Breaches and Failures in the U.S. Government," Heritage Foundation *Backgrounder* No. 2695, May 24, 2012, http://www.heritage.org/research/reports/2012/05/the-alarming-trend-of-cybersecurity-breaches-and-failures-in-the-us-government.

[3] Hearing, "Cybersecurity, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland," Homeland Security and Governmental Affairs Committee, U.S. Senate, 113th Congress, 2nd Session, September 10, 2014, http://www.cq.com/doc/congressionaltranscripts-4544717?3 (accessed October 20, 2014).

[4] Seth Rosenblatt, "Nuclear Regulator Hacked 3 Times in 3 Years," CNET, August 18, 2014, http://www.cnet.com/news/nuclear-commission-hacked-3-times-in-3-years/ (accessed October 10, 2014).

[5] Brian Honea, "Virginia Man Sentenced for Hacking Fannie Mae-Run Website," DSNews, October 10, 2014, http://dsnews.com/news/10-10-2014/virginia-man-sentenced-hacking-fannie-mae-run-website (accessed October 15, 2014).

[6] Brian Brewin, "Hacker Attacks Defense Pharmacy Site," Nextgov, January 24, 2011, http://www.nextgov.com/health/2011/01/hacker-attacks-defense-pharmacy-site/48356/ (accessed October 15, 2014).

[7] Press Release, "NOAA National Weather Service Employee Indicted for Allegedly Downloading Restricted Government Files," U.S. Attorney's Office for the Southern District of Ohio, October 20, 2014, http://www.fbi.gov/cincinnati/press-releases/2014/noaa-national-weather-service-employee-indicted-for-allegedly-downloading-restricted-government-files (accessed October 21, 2014).

[8] Siobhan Gorman, "Iranian Hacking to Test NSA Nominee Michael Rogers; Infiltration of Navy Computer Network More Extensive than Previously Thought," *Wall Street Journal (Online)*, February 18, 2014, http://online.wsj.com/news/articles/SB10001424052702304899704579389402826681452?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424052702304899704579389402826681452.html (accessed March 31, 2013).

- The Plans and Analysis Integration Office in which the hackers accessed defense program budgeting data, among other materials;

- The Fort Monmouth Army Corps Engineer Research and Development Center where the hackers obtained classified Army Corps documents, including plans for the demolition and disposal of military facilities. The center was attacked again two months later by the same hackers who used the same vulnerabilities to access massive amounts of personal, command, control, and intelligence data;

- The Army War College's Strategic Studies Institute in which the hackers accessed unspecified data multiple times over several months; and

- The Missile Defense Agency from which the hackers stole the personal information of over 4,000 individuals.[9]

7. **DOD Payroll, March 2012–June 2013.** Several men who participated in an international cybercrime ring have been charged with hacking the DOD's payroll service and other private financial companies. While it is unclear how many individuals were affected, the government "has so far identified attempts to defraud the victim companies and their customers of more than $15 million."[10]

U.S. Department of Energy (DOE)

8. **DOE, October 2013.** The DOE Office of the Inspector General (IG) report for fiscal year (FY) 2013 found that one DOE site had 11 server systems and devices that were configured with either weak password protection or no protection at all. These vulnerabilities left the devices open to attack and unauthorized access that could have allowed attackers to access and harm other internal DOE networks. Another DOE site had seven payroll servers configured with open access and no password protection that could have allowed remote or rogue systems to access sensitive personal and financial information. In total, across the DOE, the IG found 29 new weaknesses and 10 unresolved weaknesses that had been identified the previous year.[11]

9. **DOE Server, July 2013.** In December 2012, the hacker group Anonymous exploited Adobe's ColdFusion software to plant "back doors" in DOE servers. The hackers were able to repeatedly access the server and by July 2013 had stolen the personal information of between 104,000 and 150,000 individuals associated with the DOE, along with information on nearly 2,000 bank accounts. A federal audit later revealed that the DOE had been warned of weaknesses in its cybersecurity but had failed to act.[12]

Federal Election Commission (FEC)

10. **FEC Computer System, October 2013.** Chinese hackers crashed the FEC's computer system during the government shutdown while there were no staffers around to notice. The information the hackers accessed and the damage they caused remains undisclosed.[13]

[9] Jim Finkle and Joseph Menn, "FBI Warns of U.S. Government Breaches by Anonymous Hackers," Reuters, November 15, 2013, http://www.reuters.com/article/2013/11/15/us-usa-security-anonymous-fbi-idUSBRE9AE17C20131115 (accessed October 20, 2014), and Darren Pauli, "Aussies Hacked Pentagon, US Army, and Others," itnews, October 29, 2013, http://www.itnews.com.au/News/362202,aussies-hacked-pentagon-us-army-and-others.aspx (accessed October 20, 2014).

[10] Press Release, "Two Admit Roles in Multimillion-Dollar International Cybercrime Scheme," U.S. Attorney's Office, District of New Jersey, May 20, 2014, http://www.justice.gov/usao/nj/Press/files/Gundersen,%20Richard,%20and%20Taylor,%20Lamar%20Plea%20PR.html (accessed October 20, 2014).

[11] U.S. Department of Energy, Office of Inspector General, *The Department of Energy's Unclassified Cyber Security Program—201*, DOE/IG-0897, October 2013, http://energy.gov/sites/prod/files/2013/11/f4/IG-0897.pdf (accessed April 14, 2014).

[12] Finkle and Menn, "FBI Warns of U.S. Government Breaches," and Privacy Rights Clearinghouse, "Chronology of Data Breaches," http://www.privacyrights.org/data-breach/new (accessed March 25, 2014).

[13] "Report: Chinese Hackers Attacked Crucial Government Election Website," CNN, December 17, 2013, http://politicalticker.blogs.cnn.com/2013/12/17/report-chinese-hackers-attacked-crucial-government-election-website/ (accessed March 25, 2014).

Internal Revenue Service (IRS)

11. **IRS, April 2014.** An April 2014 Government Accountability Office (GAO) report found that the IRS had "not always effectively implemented access and other controls to protect the confidentiality, integrity, and availability of its financial systems and information." The GAO concluded that financial and taxpayer information remained vulnerable to unauthorized access or threat. The IRS failed to install and update security patches, monitor database controls, and restrict mainframe access.[14]

12. **IRS Website, July 2013.** The social security numbers of multiple individuals were exposed on the IRS website.[15]

National Aeronautics and Space Administration (NASA)

13. **NASA Server, July 2013.** Lauri Love, a British man, and unnamed co-conspirators connected to the hacker group Anonymous exploited flaws in the NASA server's Adobe's ColdFusion software and accessed numerous personal files.[16]

U.S. Department of Health and Human Services (HHS)

14. **Healthcare.gov, August 2014.** An unknown hacker breached the HHS server and placed malicious software on it in July. The breach was discovered in August. There was no evidence that any consumer information was taken.[17]

15. **Healthcare.gov, October 2013–January 2014.** In addition to the much-maligned rollout of Healthcare.gov, multiple serious security flaws and vulnerabilities were found. One of these allowed hackers to reset users' passwords and gain access to their accounts. It took over three weeks before the vulnerabilities were corrected.[18] Multiple cyber experts warned Congress,[19] and the Centers for Medicare and Medicaid Services' chief cybersecurity official revealed that HHS had been warned of possible security flaws before the website was launched.[20] Additional vulnerabilities were found in the "data-set" feature of Healthcare.gov in January 2014 that allowed spam or potentially malicious external websites to advertise on Healthcare.gov. [21]

U.S. Environmental Protection Agency (EPA)

16. **The FedCenter, January 2012.** Lauri Love, a British man, and unnamed co-conspirators connected to the hacker group Anonymous exploited weaknesses in the FedCenter's server through its Adobe ColdFusion software. The hackers stole hundreds of megabytes of employees' personal information.[22]

U.S. Office of Personnel Management (OPM)

17. **OPM Computer Systems, March 2014.** A Chinese hacker penetrated the computer systems of the OPM. It is unknown if any personal informa-

[14] Government Accountability Office, *Information Security: IRS Needs to Address Control Weaknesses That Place Financial and Taxpayer Data at Risk*, GAO–14–405, April 2014, http://www.gao.gov/assets/670/662371.pdf (accessed April 14, 2014).

[15] Privacy Rights Clearinghouse, "Chronology of Data Breaches."

[16] Finkle and Menn, "FBI Warns of U.S. Government Breaches," and Pauli, "Aussies Hacked Pentagon, US Army, and Others."

[17] Denver Nick, "Obamacare Website Was Hacked in July," *Time*, September 4, 2014, http://time.com/3270936/obamacare-website-was-hacked-in-july/ (accessed October 6, 2014).

[18] Jose Pagliery, "Security Hole Found in Obamacare Website," CNN, October 29, 2013, http://money.cnn.com/2013/10/29/technology/obamacare-security/index.html?section=money_technology (accessed April 9, 2014).

[19] Elizabeth Harrington, "Hearing: Security Flaws in Obamacare Website Endanger Americans," *Washington Free Beacon*, November 19, 2013, http://freebeacon.com/issues/hearing-security-flaws-in-obamacare-website-endanger-americans/ (accessed April 9, 2014).

[20] Devin Dwyer, "Exclusive: Security Risks Seen at HealthCare.gov Ahead of Sign-Up Deadline," ABC News, December 20, 2013, http://abcnews.go.com/blogs/politics/2013/12/exclusive-security-risks-seen-at-healthcare-gov-ahead-of-sign-up-deadline (accessed April 9, 2014).

[21] Jeryl Bier, "Opportunistic Marketers Exploit Opening at Healthcare.gov," January 23, 2014, http://www.weeklystandard.com/blogs/opportunistic-marketers-exploit-opening-healthcaregov_775259.html (accessed April 10, 2014).

[22] Finkle and Menn, "FBI Warns of U.S. Government Breaches," and Pauli, "Aussies Hacked Pentagon, US Army, and Others."

tion was stolen, but the network contained information on all federal employees and applicants who applied for top-secret security clearances.[23]

Central Intelligence Agency (CIA)

18. **CIA Official Website, February 2012.** The group known as Anonymous claimed responsibility for shutting down the CIA's homepage for a day.[24]

U.S. Department of Veterans Affairs (VA)

19. **E-Verify, January 2014.** A software glitch in the VA's E-Verify system exposed users' personal information to almost anyone with access to the system. The banking, medical, and military records of more than 5,300 users may have been affected.[25]

Department of Education (DOE)

20. **DOE Networks, 2013.** The DOE Inspector General's (IG) report for FY 2013 found the DOE was using unsecured networks. The IG reported that DOE was consistently not following IT security configuration procedures established by the National Institute of Standards and Technology, which meant that security patches often went without updates. The absence of proper security updates leaves the DOE networks unsecure and "increases the risks that unauthorized activities may occur and increases the potential that sensitive Department data may be released, used, or modified." IG audit testers were able to successfully connect a rogue computer to the DOE headquarters network and access sensitive information unnoticed. This same issue was identified in the 2011 and 2012 IG reports but had not been corrected.[26]

U.S. Federal Courts

21. **Federal Court System, January 2014.** A denial of service attack disabled PACER (the courts' electronic filing system), uscourts.gov, and several other Federal Court websites. The European Electronic Army claimed responsibility for the attack.[27]

Unspecified Government Agencies

22. **Microsoft XP, April 2014.** Federal officials have known for over 6 years that Microsoft was going to end its support for Windows XP in April 2014. Despite that and a recent rush to upgrade government computers, about 10 percent of the 7 million computers used by the federal government still operated using Windows XP after public support ended. The use of XP is spread throughout government agencies, including classified military and diplomatic systems. Without the software support and security updates from Microsoft, hundreds of thousands of government computers are left vulnerable if they do not upgrade or purchase special support from Microsoft.[28]

[23] Michael S. Schmidt, David E. Sanger, and Nicole Perlroth, "Chinese Hackers Pursue Key Data on U.S. Workers," *The New York Times*, July 9, 2014, http://www.nytimes.com/2014/07/10/world/asia/chinese-hackers-pursue-key-data-on-us-workers.html?hp&action=click&pgtype=Homepage&version=LedeSum&module=first-column-region&region=top-news&WT.nav=top-news&_r=1 (accessed October 3, 2014).

[24] "Anonymous Says Attack Put CIA Website Offline," BBC News, February 11, 2012, http://www.bbc.co.uk/news/world-us-canada-16993488 (accessed October 10, 2014).

[25] Josh Hicks, "VA Software Glitch Exposed Veterans' Personal Information," *The Washington Post,* January 22, 2014, http://www.washingtonpost.com/blogs/federal-eye/wp/2014/01/22/va-software-glitch-exposed-veterans-personal-information (accessed March 24, 2014).

[26] U.S. Department of Education, Office of Inspector General, *The U.S. Department of Education's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2013*, ED-OIG/A11N0001, November 2013, p. 10, http://www2.ed.gov/about/offices/list/oig/auditreports/fy2014/a11n0001.pdf (accessed April 10, 2014).

[27] Brian Fung, "Online Outage Cripples U.S. Court System," *The Washington Post*, January 24, 2014, http://www.washingtonpost.com/blogs/the-switch/wp/2014/01/24/online-attack-cripples-u-s-court-system (accessed March 25, 2014).

[28] Craig Timberg and Ellen Nakashima, "Government Computers Running Windows XP Will Be Vulnerable to Hackers after April 8," March 16, 2014, http://www.washingtonpost.com/business/technology/government-computers-running-windows-xp-will-be-vulnerable-to-hackers-after-april-8/2014/03/16/9a9c8c7c-a553-11e3-a5fa-55f0c77bf39c_story.html (accessed April 10, 2014), and Ina Fried, "Some Businesses, Governments Still Getting XP Support From Microsoft, for a Hefty Price," re/code, April 9, 2014, http://recode.net/2014/04/09/some-businesses-governments-still-getting-xp-support-from-microsoft-for-a-hefty-price/ (accessed October 23, 2014).

23. **Federal Agencies, April 2014.** An April 2014 GAO report found that reported security incidents involving personally identifiable information from federal agencies more than doubled over the past several years to 25,566 in 2013. The report also found that "agencies have had mixed results in addressing the eight components of an information security program called for by law, and most agencies had weaknesses in implementing specific security controls." Further, the GAO discovered that none of the agencies studied "consistently documented lessons learned from their breach responses."[29]

First: Do No Harm

These hacks, plus other classified, undisclosed, or unknown cyber breaches and failures, clearly demonstrate that the government has not mastered cybersecurity. Government cybersecurity rules and regulations have been in place for years, but breaches and failures continue. Imposing stringent regulation on the private sector would likely harm innovation, result in costly rules, and create a compliance mindset rather than a security mindset. Before considering such regulations, the U.S. should pursue a variety of policies that empower the private sector and encourage real collaboration among the public and private sectors.

Congress and the Administration should:

- **Enhance the sharing of cyber threat and vulnerability information.** The private sector has a great deal of information and experience to contribute to U.S. cybersecurity efforts. To enable the flow of information, the government should provide strong liability, regulatory use, and Freedom of Information Act protections to sharers. Additionally, it should form a public-private partnership organization to act as a hub for timely information sharing between the government and the private sector.[30]
- **Lead international efforts to respond to cyber aggression.** The government should take a leading international role in punishing malicious cyber nations and bad cyber actors. The U.S. should name and shame cyber aggressors, cease military and cyber cooperation with them, take legal action against foreign companies trafficking in stolen information or property, pursue trade and visa-related consequences, and consider greater support for democratic movements and Internet freedom in countries that are the most aggressive bad actors.

Cybersecurity for All

These breaches of government security as well as the many high-profile private-sector failures demonstrate that no cybersecurity system is perfect: There is no silver bullet. However, the U.S. can take simple and low-cost steps such as information sharing to improve public and private cybersecurity efforts. Such steps, along with reforms in cybersecurity insurance, supply chain security, and cyber workforce development, can make the U.S. more secure in cyberspace.

*—**David Inserra** is Research Associate for Homeland Security and Cybersecurity in the Douglas and Sarah Allison Center for Foreign and National Security Policy, of the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, at The Heritage Foundation. **Paul Rosenzweig** is a Visiting Fellow in the Allison Center.*

[29] U.S. Government Accountability Office, *Information Security: Federal Agencies Need to Enhance Responses to Data Breaches*, GAO–14–487T, April 2, 2014, http://gao.gov/assets/670/662227.pdf (accessed April 10, 2014).

[30] For a more detailed summary of our views on this, see Steven P. Bucci, Paul Rosenzweig, and David Inserra, "A Congressional Guide: Seven Steps to U.S. Security, Prosperity, and Freedom in Cyberspace," Heritage Foundation *Backgrounder* No. 2785, April 1, 2013, http://www.heritage.org/research/reports/2013/04/a-congressional-guide-seven-steps-to-us-security-prosperity-and-freedom-in-cyberspace; David Inserra and Paul Rosenzweig, "Cybersecurity Information Sharing: One Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace," Heritage Foundation *Backgrounder* No. 2899, April 1, 2013, http://www.heritage.org/research/reports/2014/04/cybersecurity-information-sharing-one-step-toward-us-security-prosperity-and-freedom-in-cyberspace; and David Inserra, "Senate Cyber Information-Sharing Bill on the Right Track but Improvements Needed," Heritage Foundation *Issue Brief* No. 4269, September 2, 2014, http://www.heritage.org/research/reports/2014/09/senate-cyber-information-sharing-bill-on-the-right-track-but-improvements-needed.