The Heritage Foundation
LEADERSHIP FOR AMERICA

ISSUE BRIEF

No. 3772 | NOVEMBER 13, 2012

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

Paul Rosenzweig

This summer, the Cybersecurity Act of 2012 (CSA) failed to pass the Senate, with Democrats and Republicans alike voting against the bill. The overriding concern was that the regulatory approach of the bill would be ineffective at best and harmful at worst.

Following the failure of the CSA, the Obama Administration began drafting a cybersecurity executive order that is based on regulations, similar to the CSA. While the CSA and the executive order see government-designed standards and regulations as the way to encourage cybersecurity, the performance of the federal government in securing its own computer systems calls such an approach into question.

Many government agencies are known to have flawed cybersecurity practices, yet despite the best efforts of those creating the standards for these agencies, these organizations often remain vulnerable. Instead of relying on a static, top-down government approach to cybersecurity, the U.S. should have a dynamic solution that leverages the strengths of both the government and the private sector.

What follows is list of federal government cybersecurity breaches and failures since May 2012. The compilation of this list (or any list, for that matter) necessarily requires judgment in determining whether an incident qualifies for the list. This list is by no means complete: Some hacks might not be reported, and others have not even been realized yet. Additionally, the list does not include the large number of private-sector failures. Nevertheless, the seriousness and amount of U.S. government cybersecurity failures undercut the argument for a government-led regulatory approach to cybersecurity. The list is alphabetical by agency.

U.S. Army Chief of Public Affairs

1. **Awards Database—September 2012.** A contractor erroneously uploaded an Army awards database to a public server. This breach made the personal records of over 500 Army personnel available, including some Social Security numbers.[1]

Commodity Futures Trading Commission (CFTC)

2. **E-mail System—June 2012.** An employee of the CFTC was fooled by a phishing e-mail and gave away sensitive information to unknown hackers. The hacker was able to use this information to access the employee's e-mails and attachments, which contained sensitive information, including Social Security numbers for up to 700 employees of the CFTC.[2]

U.S. Department of Energy (DOE)

3. **National Energy Research Scientific Computer Center—June 2012.** James Miller of Devon, Pennsylvania, broke into a DOE supercomputer and was able to use it for his own purposes. He was noticed only because he tried to sell access to an undercover FBI agent.[3]

U.S. Department of Health and Human Services

This paper, in its entirety, can be found at **http://report.heritage.org/ib3772**

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

4. **Databases at the Centers for Medicare and Medicaid Services (CMS)—September 2009–December 2011.** CMS was breached 13 times by unknown hackers, affecting over 300 records. The CMS did not notify the affected parties in a timely manner for seven of these breaches. Additionally, the CMS notification did not provide critical information regarding the type of information exposed or when the breach occurred.[4]

U.S. Department of Homeland Security (DHS)

5. **DHS website—June 2012.** A hacker group calling itself "digital-corruption" hacked a DHS website and stole personal data including usernames, passwords, and security questions and answers.[5]

U.S. Department of Justice (DOJ)

6. **DOJ websites—May 2012.** The hacker group Anonymous hacked the Bureau of Justice Statistics and stole 1.7 gigabytes of data, which it proceeded to publish online. The hacked data included internal e-mails that likely contained personal or sensitive information related to crimes, criminals, or crime victims.[6]

U.S. Environmental Protection Agency (EPA)

7. **EPA Superfund servers—March 2012.** The EPA was breached by an unknown hacker and lost personal and financial information including Social Security numbers, bank account numbers, and addresses belonging to almost 8,000 users. The breach is thought to have come through a virus on a contractor's computer, but that has not been confirmed.[7]

Federal Retirement Thrift Investment Board

8. **Thrift Savings Plan Database—May 2012.** An unknown hacker stole personal and financial information including Social Security numbers, addresses, and account numbers from thousands of individuals, likely through a contractor's computer.[8]

National Weather Service (NWS)

9. **NWS website and servers—October 2012.** A hacker group known as "Kosova Hacker's Security" breached the NWS's website and posted lists of files, vulnerability information, and administrators' account names. The hackers claim to be motivated by U.S. action against Muslim nations, specifically the Stuxnet and Flame malware.[9]

U.S. Navy

10. **Navy website—June 2012.** A hacker known as ".c0mrad" broke into the U.S. Navy's public website and downloaded over 170 military e-mails and passwords.[10]

11. **Navy website—June 2012.** A hacker group calling itself

1. Privacy Rights Clearinghouse, "Chronology of Data Breaches," http://www.privacyrights.org/data-breach/new (accessed November 5, 2012).
2. Silla Brush, "CFTC Data Breach Risks Employees' Social Security," Bloomberg News, June 25, 2012, http://www.businessweek.com/news/2012-06-25/cftc-data-breach-risks-employees-social-security-numbers (accessed November 5, 2012).
3. Mathew J. Schwartz, "Feds Bust Hacker for Selling Government Supercomputer Access," *Information Week*, June 21, 2012, http://www.informationweek.com/security/attacks/feds-bust-hacker-for-selling-government/240002474 (accessed November 5, 2012).
4. Privacy Rights Clearinghouse, "Chronology of Data Breaches."
5. Adam Jones, "Another US Government Site Hacked!," *Security*, June 23, 2012, http://www.seczine.com/article/hacking-news/230612/another-us-gov-site-hacked.php (accessed November 5, 2012).
6. John Ribeiro, "Anonymous Claims It Hacked a Justice Department Site," *PCWorld*, May 23, 2012, http://www.pcworld.com/article/256034/anonymous_claims_it_hacked_a_doj_site.html (accessed November 5, 2012).
7. Amber Corrin, "Was the EPA Data Breach a Failure of Cybersecurity 101?," FCW, August 3, 2012, http://fcw.com/articles/2012/08/03/epa-security-breach-contractors-virus.aspx (accessed November 5, 2012).
8. Eric Yoder, "TSP Discloses Hacking of Accounts," *The Washington Post*, May 25, 2012, http://www.washingtonpost.com/blogs/federal-eye/post/tsp-discloses-hacking-of-accounts/2012/05/25/gJQAsM4kpU_blog.html (accessed November 5, 2012).
9. Paul Roberts, "National Weather Service Website Hacked by Kosova Hacker's Security," Nakedsecurity, October 19, 2012, http://nakedsecurity.sophos.com/2012/10/19/national-weather-service-website-hacked-by-kosovo-hackers-security/ (accessed November 5, 2012).
10. Gianluca Messofiore, "Hacker Comrade Attacks US Navy Website and Leaks Personal Military Emails and Passwords," *International Business Times*, http://www.ibtimes.co.uk/articles/347819/20120601/c0mrade-navy-emails-hacker-anonymous-habbo-freemasons.htm (accessed November 5, 2012).

"digital-corruption" hacked the Navy website and stole personal data including usernames, passwords, and security questions and answers.[11]

12. Navy Smart Web Move Database—September 2012. An unknown hacker or hackers breached a database containing the sensitive data of over 200,000 people. It is unknown exactly how much was stolen, but many usernames and security questions and answers were taken.[12]

U.S. Office of Personnel Management (OPM)

13. OPM Database—May 2012. An unknown hacker broke into the OPM database and posted the stolen information online. Thirty-seven user IDs and passwords were compromised.[13]

*—**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. David Inserra, a Research Assistant in the Allison Center, contributed to this report.*

11. Jones, "Another US Government Site Hacked!"
12. Mike Hixenbaugh, "Hackers Get Personal Data from Navy Website," *The Virginian-Pilot*, September 21, 2012, http://hamptonroads.com/2012/09/hackers-get-personal-data-navy-website (accessed November 5, 2012).
13. Privacy Rights Clearinghouse, "Chronology of Data Breaches."