The Heritage Foundation
LEADERSHIP FOR AMERICA

ISSUE BRIEF

No. 3968 | JUNE 13, 2013

Government Cyber Failures Reveal Weaknesses of Regulatory Approach to Cybersecurity

Paul Rosenzweig and David Inserra

Last year, the Senate twice voted down the Cybersecurity Act of 2012 because of concerns that a regulatory approach might harm U.S. cybersecurity efforts. Despite these concerns, President Obama issued a cybersecurity executive order that uses a regulatory or standards-based approach to require additional security from private-sector organizations. The government, however, already requires its own agencies to follow existing cybersecurity standards. The best way to see the effectiveness of cybersecurity standards is to observe how well the government has handled its own security guidelines.

The following is a list of federal government cybersecurity breaches and failures since November 2012. This list is in no way complete: Some hacks might not be reported, and others have yet to be realized. Furthermore, the list 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.

This paper, in its entirety, can be found at
http://report.heritage.org/ib3968

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

Department of Defense (DOD)

1. **U.S. Army Corps of Engineers' national inventory of dams, May 2013.** Hackers breached databases across the United States, compromising non-public information (including vulnerabilities) of approximately 8,100 major dams.[1]

2. **Pentagon, April 2013.** An unspecified breach compromised 500,000 e-mails from a Pentagon drive. This breach made it possible for Guantanamo prosecutors to see confidential defense files.[2]

3. **Army National Guard website, March 2013.** The Tunisian Cyber Army, in conjunction with the al-Qaeda Electronic Army and Chinese hackers, hacked the Army National Guard's website. All parties involved were able to obtain important DOD documents.[3]

4. **U.S. Army Fort Monmouth, December 2012.** Hackers breached a database with massive amounts of data. Personal information (including Social Security numbers) of personnel and visitors was exposed. Information from Command, Control, Communications, Intelligence, Surveillance and Reconnaissance was accessed as well.[4]

U.S. Department of Energy (DOE)

5. **Servers and workstations, January 2013.** Hackers exploited a vulnerability that the DOE had been aware of since 2012, infecting 14

servers and 20 workstations and exposing several hundred employees' personal information.[5]

Department of Homeland Security (DHS)

6. **Personal information, April 2013.** Hackers stole Social Security and financial information of the newly appointed director of the Secret Service and posted it on the Internet.[6]

7. **Background investigations, May 2013.** DHS has recently learned of a vulnerability that existed in the software used by a vendor to process personnel security investigations. As a result, the personal information (such as names, date of birth, and Social Security numbers) of tens of thousands of employees and DHS clearance holders was potentially accessible to unauthorized users.[7]

U.S. Department of Labor (DOL)

8. **DOL website, April 2013.** Hackers placed malicious code on the DOL's website. This code then infected computers that visited the site.[8]

Department of State (DOS)

9. **DOS website, March 2013.** The Tunisian Cyber Army, in conjunction with the al-Qaeda Electronic Army, exploited a weakness on the DOS website, enabling them to extract important documents. They claim to have sensitive information of government computers and servers.[9]

10. **DOS website, February 2013.** The hacker group Anonymous gained access to a DOS database through the department's website. The group then published the contents online.[10]

Federal Communications Commission

11. **Emergency Alert System (EAS), February 2013.** Hackers infiltrated EAS systems across the nation and sent a message alerting people to a fictitious zombie attack. EAS officials changed all passwords and double-checked all firewalls before bringing the EAS back online.[11]

Federal Reserve

12. **Internal websites, February 2013.** Anonymous gained access to the internal websites through a vulnerability in a website vendor product. This allowed them to steal information on more than 4,000 bank executives.[12]

General Services Administration

13. **System for Award Management (SAM),**

1. Privacy Rights Clearinghouse, "Chronology of Data Breaches," http://www.privacyrights.org/data-breach/new (accessed June 6, 2013).
2. Ibid.
3. RT, "Al-Qaeda Electronic Army Continues Assault on US Government Websites," March 12, 2013, http://rt.com/usa/qaeda-tunisia-cyber-army-175/ (accessed June 6, 2013).
4. Privacy Rights Clearinghouse, "Chronology of Data Breaches."
5. Ibid.
6. Carol Cratty, "Secret Service Head Personal Info on Internet, Site Claims," CNN, April 4, 2013, http://www.cnn.com/2013/04/04/politics/secret-service-director-personal (accessed June 6, 2013).
7. U.S. Department of Homeland Security, "Privacy Response to Potential PII Incident," http://www.dhs.gov/pii (accessed June 6, 2013).
8. Jennifer LeClaire, "Labor Department Web Site Hacked, Malware Uploaded," CIO Today, May 1, 2013, http://www.cio-today.com/story.xhtml?story_id=0020000623MG&full_skip=1 (accessed June 6, 2013).
9. RT, "Electronic Al-Qaeda Army Claims to Have Hacked US Government Websites," March 11, 2013, http://rt.com/usa/hacked-us-government-websites-112/ (accessed June 6, 2013).
10. Mark Hoffman, "Cyberwar: Anonymous Hacked U.S. Government Multiple Times," *Science World Report*, February 25, 2013, http://www.scienceworldreport.com/articles/5170/20130225/cyberwar-anonymous-hacked-us-government-multiple-times.htm (accessed June 6, 2013).
11. Privacy Rights Clearinghouse, "Chronology of Data Breaches."
12. Reuters, "Federal Reserve Hacked," *The Guardian*, February 6, 2013, http://www.guardian.co.uk/business/2013/feb/06/federal-reserve-anonymous (accessed June 6, 2013).

March 2013. A security vulnerability allowed SAM users to see the financial information of other SAM users. It is unclear how long the vulnerability was in the system.[13]

National Aeronautics and Space Administration (NASA)

14. **Laptop and sensitive documents stolen, November 2012.** Thieves broke into a NASA employee's car and stole a NASA laptop and sensitive NASA documents. The information of employees, contractors, and other non-employees was exposed.[14]

National Institute of Standards and Technology (NIST)

15. **National Vulnerability Database (NVD), March 2013.** Hackers gained access to NIST's database through a software vulnerability. After the database was offline for about a week, officials traced the malware to two web servers. It does not look as if the NVD website distributed malware to users who visited the site.[15]

U.S. Sentencing Commission

16. **U.S. Sentencing Commission website, January 2013.** Protesting the prosecution of programmer and hacktivist Aaron Swartz, Anonymous seized control of the U.S. Sentencing Commission website. The group posted a playable version of the video game *Asteroids* on the commission's website.[16]

A Different Approach to Cybersecurity

The list above is ample reason to be skeptical of the government's ability to manage cybersecurity standards. Such standards have the potential to harm the private sector by creating a culture of compliance, harming innovation, and ignoring cost-effective solutions. Instead of a top-down regulatory approach, 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 that it can 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.

- **Foster the development of cyber supply chain ratings.** Dangerous cyber threats to both the government and the private sector can come from malicious hardware. Encouraging the creation of cyber supply chain ratings from a nonprofit organization would help both the private and public sectors determine the security of cyber components. This would allow companies to make careful risk-based decisions regarding their cybersecurity.

- **Lead international cyber engagement.** The government should take a leading international role by making bad cyber actors feel more pain when they act maliciously. The U.S. should name and shame bad actors, cease military and cyber cooperation with them, and take legal action against foreign companies trafficking in stolen information or property.

Rejecting Flawed Cyber Regulations

The government's many cyber breaches and failures demonstrate that regulations, standards, and rules do not guarantee security. Rather than impose these standards on the private sector, Congress should pursue cybersecurity policies that are flexible, cost-effective, and risk-based.

13. Privacy Rights Clearinghouse, "Chronology of Data Breaches."
14. Ibid.
15. Grant Gross, "U.S. NIST's Vulnerability Database Hacked," *Computer World*, March 14, 2013, http://www.computerworld.com/s/article/9237605/U.S._NIST_s_vulnerability_database_hacked (accessed June 6, 2013).
16. Alex Johnston, "Anonymous Hacks Government Website, Posts Game of 'Asteroids,'" *Epoch Times*, January 28, 2013, http://www.theepochtimes.com/n2/united-states/anonymous-hacks-government-website-posts-game-of-asteroids-341295.html (accessed June 6, 2013).

—***Paul Rosenzweig*** *is a Visiting Fellow in the Center for Legal and 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, and* ***David Inserra*** *is a Research Assistant in the Allison Center, at The Heritage Foundation.* *The authors are grateful to interns Sarah Friesen and Elizabeth Simson for their help in preparing this paper.*