The Heritage Foundation

ISSUE BRIEF

No. 4804 | JANUARY 3, 2018

Federal Cyber Breaches in 2017

Riley Walters

While mega-breaches of high-profile private companies are the norm for headline fodder, the federal government also has its share of vulnerabilities in cyberspace. A February 2017 report by the Government Accountability Office (GAO) highlights the federal government's consistent shortcomings when it comes to protecting federal information systems.[1] The GAO highlights the need for agencies to improve their cyber incident detection, response, and mitigation, and better protect personally identifiable information. The breach of the Office of Personnel Management (OPM) in 2015 and theft of 22 million personnel records by Chinese hackers is no less proof of the need for greater security.

Yet agencies continue to be plagued by cyber incidents. In fiscal year (FY) 2016, government agencies reported 30,899 information security incidents, 16 of which met the threshold of being a major incident.[2] A second report by the GAO, released in September 2017, highlighted federal agencies' continued weakness in protecting their information systems.[3] At least 21 agencies continued to show weakness in the five major categories for information-security control: access, configuration management, segregation of duties, contingency planning, and agency-wide security management.

This paper, in its entirety, can be found at
http://report.heritage.org/ib4804

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

This *Issue Brief* is a continuation in a series of papers that highlight cyber incidents involving the federal government between 2004[4] and 2015.[5] Incidents are listed in chronological order by the date the incident is first reported to the public and does not necessarily reflect the time the breach originally occurred.

November 2016

Department of the Navy.[6] The Navy was notified in October 2016 that a laptop containing the names and social security numbers of 134,386 current and former sailors was compromised.[7] The laptop belonged to an employee of Hewlett Packard Enterprise Services which serves as a Navy contractor.

December 2016

Election Assistance Commission (EAC).[8] Recorded Future, a threat intelligence firm, came across a Russian-speaking hacker looking to sell more than 100 potentially compromised access credentials of the EAC database.[9] Some of the credentials contained administrative privileges. The hacker, given the name Rasputin, has no known affiliation to a foreign government and claims to have breached the EAC system. According to Recorded Future, Rasputin was in negotiations to sell the information to a buyer working on behalf of a Middle Eastern government. In February 2017, Recorded Future found Rasputin attempting to sell unauthorized access to a number of state and federal agencies though there was no sign of an actual breach.[10]

January 2017

Department of Defense (DOD). Not all breaches are malicious. Since March 2016 the DOD and

HackerOne—a bug bounty platform—have initiated a series of "Hack the Pentagon" campaigns.[11] The campaigns allow U.S.-based hackers to hunt for vulnerabilities in the DOD's public-facing networks in exchange for a reward. During a Hack the Pentagon campaign that ran from November 30, 2016, to December 21, 2016, a hacker was able to access an internal DOD network through the goarmy.com website.[12] Only those with authorized access can normally access the Internet network.

March and April 2017

Central Intelligence Agency (CIA) and National Security Agency (NSA). Any public release of classified information, especially information reportedly originating from within the American intelligence community, should err on the side of caution when recognizing its authenticity. In March 2017, Wikileaks released what it believes to be a list of CIA hacking tools.[13] The list, known as "Year Zero" or "Vault 7," was reportedly acquired by Wikileaks while the information was being passed between government employees and contractors in an "unauthorized manner."[14] A month later, a group known as the Shadow Brokers continued releasing what it claimed to be NSA hacking tools.[15] One of the tools included, known as EternalBlue, was associated with a number of cyber attacks that occurred throughout the summer of 2016.[16] The Shadow brokers claim to have stolen these tools from a team reportedly associated with the NSA, known as the "Equation Group."

Internal Revenue Service (IRS). The Data Retrieval Tool for the IRS's Free Application for Federal Student Aid was breached as early as September

1. Gregory C. Wilshusen, "Cybersecurity Actions Needed to Strengthen U.S. Capabilities," testimony before the Subcommittee on Research and Technology, Committee on Science, Space, and Technology, U.S. House of Representative, February 14, 2017, http://www.gao.gov/assets/690/682756.pdf (accessed December 4, 2017).
2. Office of Management and Budget, Federal Information Security Modernization Act of 2014, *Annual Report to Congress, 2016*, November 2016, https://www.whitehouse.gov/sites/whitehouse.gov/files/briefing-room/presidential-actions/related-omb-material/fy_2016_fisma_report%20to_congress_official_release_march_10_2017.pdf (accessed December 4, 2017).
3. Government Accountability Agency, "Federal Information Security Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices," Report to Congressional Committees, September 2017, http://www.gao.gov/assets/690/687461.pdf (accessed December 4, 2017).
4. Paul Rosenzweig and David Inserra, "Breaches Warn Against Cybersecurity Regulation," Heritage Foundation *Issue Brief* No. 4288, October 27, 2014, http://www.heritage.org/defense/report/continuing-federal-cyber-breaches-warn-against-cybersecurity-regulation#_ftn2.
5. Riley Walters, "Continued Federal Cyber Breaches in 2015," Heritage Foundation *Issue Brief* No. 4488, November 19, 2015, http://www.heritage.org/cybersecurity/report/continued-federal-cyber-breaches-2015.
6. While this *Issue Brief* focuses on cyber incidents that occurred in 2017, this event from 2016 is included to ensure no gaps exist in the research on the issue of cyber incidents in the federal government.
7. Chief of Naval Personnel Public Affairs, "Security Breach Notification of Sailors' PII," America's Navy, November 23, 2016, http://www.navy.mil/submit/display.asp?story_id=97820 (accessed December 4, 2017).
8. See footnote 6
9. Andrei Barysevich, "Russian-Speaking Hacker Selling Access to the US Election Assistance Commission," Recorded Future, December 15, 2016, https://www.recordedfuture.com/rasputin-eac-breach/ (accessed December 4, 2017).
10. Levi Gundart, "Russian-Speaking Hacker Sells SQLi for Unauthorized Access to Over 60 Universities and Government Agencies," Recorded Future, February 16, 2017, https://www.recordedfuture.com/recent-rasputin-activity/ (accessed December 4, 2017).
11. "Hack the Pentagon," Hackerone, https://www.hackerone.com/resources/hack-the-pentagon (accessed December 4, 2017).
12. Eduard Kovacs, "Expert Hacks Internal DOD Network via Army Website," Security Week, January 23, 2017, http://www.securityweek.com/expert-hacks-internal-dod-network-army-website (accessed December 4, 2017).
13. Roi Perez, "WikiLeaks Releases Document Trove Allegedly Containing CIA Hacking Tools," *SC Magazine UK*, March 7, 2017, https://www.scmagazineuk.com/wikileaks-releases-document-trove-allegedly-containing-cia-hacking-tools/article/642429/ (accessed December 4, 2017).
14. Ibid.
15. Adam McNeil, "ShadowBrokers Fails to Collect 1M Bitcoins—Releases Stolen Information," Malwarebytes Labs, April 10, 2017, https://blog.malwarebytes.com/cybercrime/2017/04/shadowbrokers-fails-to-collect-1m-bitcoins-releases-stolen-information/ (accessed December 4, 2017).
16. Riley Walters, "A Massive Cybersecurity Has Hit Over 150 Countries. Here's How to Protect Your Computer," The Daily Signal, May 16, 2017, http://dailysignal.com/2017/05/16/massive-cyberattack-hit-150-countries-heres-protect-computer/.

2016.[17] Approximately 100,000 individuals may have had their taxpayer information compromised. Until the tool was turned off in March 2017, hackers were also able to file upwards of 8,000 applications[18] and steal $30 million from the U.S. government.

August 2017

Department of Labor (DOL). A new Injury Tracking Application website by the Occupational Safety and Health Administration was suspended after the Department of Homeland Security notified the DOL of a potential compromise.[19] One company was reportedly affected by the breach.

September 2017

Securities and Exchange Commission (SEC). The SEC's Electronic Data Gathering, Analysis, and Retrieval (EDGAR) database was compromised in 2016.[20] The system houses sensitive corporate and financial information and could be used by traders looking to gain an advantage in stock trading.

October 2017

Departments of State, Energy, Homeland Security, and Defense, the U.S. Postal Service, the National Institutes of Health, Fannie Mae, and Freddie Mac. A server belonging to the auditing firm Deloitte was compromised by a cyber attack ongoing since 2016.[21] The server contained the e-mails of an estimated 350 clients of Deloitte.

Federal Deposit Insurance Corporation (FDIC). Between 2015 and 2016, the FDIC may have suffered 54 breaches.[22] Of the 54 suspected or confirmed breaches, six were designated as a major incident and potentially compromised the personally identifiable information of 113,000 individuals.[23] Just a year earlier, high-level officials at the FDIC were reportedly hacked by agents of the Chinese government during a three-year hacking campaign that lasted between 2010 and 2013.[24]

U.S. Forces Korea and Republic of Korea (ROK) Armed Forces. A South Korean politician announced that North Korean hackers stole joint U.S.–ROK wartime operational plans in September 2017.[25] The 235 gigabytes of data stolen may have also included information on key military facilities and power plants.

November 2017

U.S. Army Intelligence and Security Command (INSCOM). UpGuard, a cybersecurity company, discovered in September 2017 an Amazon cloud storage containing data belonging to INSCOM.[26] The publically accessible cloud storage contained

17. Alfred Ng, "Hackers Use College Student Loans Tools to Steal $30 million," CNET, April 17, 2017, https://www.cnet.com/news/hackers-used-college-student-loans-tool-to-steal-30-million/ (accessed December 4, 2017).
18. Kenneth C. Corbin and Silvana Gina Garza, testimony before the Oversight and Government Reform Committee on the FAFSA Data Retrieval Tool, U.S. House of Representatives, May 3, 2017, https://oversight.house.gov/wp-content/uploads/2017/05/Corbin-Garza-IRS-joint-Statement-FAFSA-5-3.pdf (accessed December 4, 2017).
19. Tressi L. Cordaro, "OSHA Suspends ITA Due to Security Breach," *The National Law Review*, August 16, 2017, https://www.natlawreview.com/article/osha-suspends-ita-due-to-security-breach (accessed December 4, 2017).
20. "SEC Hit by Database Breach in 2016," Fedscoop, September 21, 2017, https://www.fedscoop.com/sec-hit-database-breach-2016/ (accessed December 4, 2017).
21. Nick Hopkins, "Deloitte Hack Hit Server Containing Emails from Across US Government," *The Guardian*, October 10, 2017, https://www.theguardian.com/business/2017/oct/10/deloitte-hack-hit-server-containing-emails-from-across-us-government (accessed December 4, 2017).
22. Billy Mitchell, "FDIC Breached More than 50 Times Between 2015 and 2016," Fedscoop, October 5, 2017, https://www.fedscoop.com/fdic-breached-50-times-2015-2016/ (accessed December 4, 2017).
23. Office of Inspector General, Office of Information Technology Audits and Cyber, "The FDIC's Processes for Responding to Breaches of Personally Identifiable Information," Report No. AUD-17-006, September 2017, https://www.oversight.gov/sites/default/files/oig-reports/FDICOIG-17-006AUD.pdf (accessed December 4, 2017).
24. Katie Bo Williams, "Chinese Government Likely Hacked FDIC: Report," *The Hill*, July 13, 2016, http://thehill.com/policy/cybersecurity/287561-chinese-government-likely-hacked-fdic-report (accessed December 4, 2017).
25. Bryan Harris, "North Korea Hacked War Blueprint, Says Seoul Lawmaker," *Financial Times*, October 10, 2017, https://www.ft.com/content/d8bbceb0-ad64-11e7-aab9-abaa44b1e130 (accessed December 4, 2017).
26. Dan O'Sullivan, "Black Box, Red Disk: How Top Secret NSA and Army Data Leaked Online," UpGuard, November 28, 2017, https://www.upguard.com/breaches/cloud-leak-inscom (accessed December 4, 2017).

sensitive information not least including details of the DOD's battlefield intelligence platform and a virtual system used for classified communication.

Government Networks Will Continue to Need Security

A breach of the Kansas Department of Commerce exposing 5.5 million social security numbers;[27] the IRS relaxing commitments to protect taxpayers' personal information;[28] and the 21 states notified by the Department of Homeland Security that their election systems were targeted by Russian hackers[29]—these additional incidents bear out the lesson of the list above. While the incidents may not apply to the federal level or reflect an actual breach in information, they no less represent the need for greater cybersecurity. To that end, the U.S. government should:

- **Support the private sector with active cyber defense.** The private sector is key in maintaining a strong U.S. cyberspace, whether it is creating new devices, implementing best practices, developing a strong cyber workforce, or defending U.S. network systems. Lawmakers should refrain from burdening the private sector with rigid regulations, instead looking to expand the private sectors' capabilities with allowing for active cyber defense.[30]
- **Continue to work with international partners.** Cyberspace knows no borders, but cyber criminals do. And they are often located outside the U.S. The U.S. should work with international friends and allies to take cyber criminals out of cyberspace and make them answer for their crimes in the real world.

No Panacea in Cybersecurity

No silver bullet exists for the problems of cybersecurity. The U.S. government should refrain from shooting the private sector in the foot with new regulations and focus on strengthening the security of its own information.

*—**Riley Walters** is a Research Associate in the Asian Studies Center, of the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, at The Heritage Foundation.*

27. Morgan Chalfant, "Over 5 Million Social Security Numbers Exposed in Kansas Breach: Report," *The Hill*, July 20, 2017, http://thehill.com/policy/cybersecurity/343028-kansas-breach-exposed-over-5-million-social-security-numbers-report (accessed December 4, 2017).
28. News release, "Employees Sometimes Did Not Adhere to E-mail Policies, Which Increased the Risk of Improper Disclosure of Taxpayer Information," U.S. Department of the Treasury, Inspector General for Tax Administration, November 17, 2016, https://www.treasury.gov/tigta/press/press_tigta-2016-36.htm (accessed December 4, 2017).
29. Joe Uchill, "DHS Tells 21 States They Were Russia Hacking Targets Before 2016 Election," *The Hill*, September 22, 2017, http://thehill.com/policy/cybersecurity/351981-dhs-notifies-21-states-of-they-were-targets-russian-hacking?utm_source=&utm_medium=email&utm_campaign=10978 (accessed December 4, 2017).
30. Paul Rosenzweig, Steven P. Bucci, and David Inserra, "Next Steps for U.S. Cybersecurity in the Trump Administration: Active Cyber Defense," Heritage Foundation *Backgrounder* No. 3188, May 5, 2017, http://www.heritage.org/cybersecurity/report/next-steps-us-cybersecurity-the-trump-administration-active-cyber-defense.