The Federal Government's Track Record on Cybersecurity and Critical Infrastructure

A report prepared by

the Minority Staff of the Homeland Security and Governmental Affairs Committee

Sen. Tom Coburn, MD, Ranking Member

February 4, 2014

Introduction

In the past few years, we have seen significant breaches in cybersecurity which could affect critical U.S. infrastructure. Data on the nation's weakest dams, including those which could kill Americans if they failed, were stolen by a malicious intruder. Nuclear plants' confidential cybersecurity plans have been left unprotected. Blueprints for the technology undergirding the New York Stock Exchange were exposed to hackers.

Examples like those underscore for many the importance of increased federal involvement in protecting the nation's privately-owned critical infrastructure. But for one thing: Those failures aren't due to poor practices by the private sector. All of the examples below were real lapses by the federal government.

- **The Nuclear Regulatory Commission** stored sensitive cybersecurity details for nuclear plants on an unprotected shared drive, making them more vulnerable to hackers and cyberthieves.

- **The Securities and Exchange Commission** routinely exposed extremely sensitive data about the computer networks supporting the New York Stock Exchange, including NYSE's cybersecurity measures. The information the SEC exposed reportedly could be extremely useful to a hacker or terrorist who wanted to penetrate the market's defenses and attack its systems.

- Last January, hackers gained access to **U.S. Army Corps of Engineers** computers and downloaded an entire non-public database of information about the nation's 85,000 dams — including sensitive information about each dam's condition, the potential for fatalities if breached, location and nearest city.[1]

- Last February, hackers reportedly broke into the national **Emergency Broadcast System**, implemented by the **Federal Emergency Management Agency (FEMA)** and the **Federal Communications Commission (FCC)** as the federal government's tool to address Americans in case of a national emergency. The hackers caused television stations in Michigan, Montana and North Dakota to broadcast zombie attack warnings. "Civil authorities in your area have reported that the bodies of the dead are rising from their graves and attacking the living," an authoritative voice stated in the hacked broadcast message, while the familiar warning beep sounded. "Do not attempt to approach or apprehend these bodies as they are considered extremely dangerous."[2]

---

[1] Senate HSGAC Minority Staff briefing with U.S. Army Corps of Engineers officials, May 3, 2013.

[2] "Local Station Breaks Into Programming With Emergency Zombie Apocalypse Alert," Mediaite.com, February 11, 2013, http://www.mediaite.com/tv/local-montana-station-breaks-into-programming-with-emergency-zombie-apocalypse-alert/, accessed January 13, 2014; "Emergency Alert System (EAS)", FCC.gov, http://www.fcc.gov/guides/emergency-alert-system-eas.

- Last March, hackers exploited a vulnerability on web servers belonging to the **National Institute of Standards and Technology (NIST)**, the federal government's authority for federal and private-sector cybersecurity. The servers, which hosted the federal government's database of known software vulnerabilities, had to be taken out of service for several days.[3]

In addition, hackers have penetrated, taken control of, caused damage to and/or stolen sensitive personal and official information from computer systems at the Departments of Homeland Security, Justice, Defense, State, Labor, Energy, and Commerce; NASA; the Environmental Protection Agency; the Office of Personnel Management; the Federal Reserve; the Commodity Futures Trading Commission; the Food and Drug Administration; the U.S. Copyright Office; and the National Weather Service, according to public reporting.[4]

These are just hacks whose details became known to the public, often because the hackers themselves announced their exploits. Largely invisible to the public and policymakers are over 48,000 other cyber "incidents" involving government systems which agencies detected and reported to DHS in FY 2012.[5] And one cannot ignore the universe of other intrusions that agencies could not detect: civilian agencies don't detect roughly 4 in 10 intrusions, according to testing reported in 2013 by the White House Office of Management and Budget.[6]

While cyber intrusions into protected systems are typically the result of sophisticated hacking, they often exploit mundane weaknesses, particularly out-of-date software. Even though they sound boring, failing to install software patches or update programs to their latest version create entry points for spies, hackers and other malicious actors. Last July, hackers used just that kind of known, fixable weakness to steal private information on over 100,000 people from the Department of Energy. The department's Inspector General blamed the theft in part on a piece

---

[3] Goodin, Dan, "National Vulnerability Database taken down by vulnerability-exploiting hack," Ars Technica, March 14, 2013, http://arstechnica.com/security/2013/03/national-vulnerability-database-taken-down-by-vulnerability-exploiting-hack/, accessed January 13, 2014.

[4] Reported incidents compiled by the Senate Committee on Commerce, 2013; Rosenzweig, Paul, "The Alarming Trend of Cybersecurity Breaches and Failures in the U.S. Government Continues," Heritage Foundation, http://www.heritage.org/research/reports/2012/11/cybersecurity-breaches-and-failures-in-the-us-government-continue, accessed January 13, 2014; Ryan, Jason, "Anonymous Hits Federal Reserve in Hack Attack," ABCNews.com, Feb. 6, 2013, http://abcnews.go.com/blogs/politics/2013/02/anonymous-hits-federal-reserve-in-hack-attack/, accessed January 13, 2014; Lennon, Mike, "NASA Inspector General Said Hackers Had Full Functional Control Over NASA Networks," SecurityWeek, March 3, 2012, http://www.securityweek.com/nasa-inspector-general-said-hackers-had-full-functional-control-over-nasa-networks, January 13, 2014; Lowenson, Josh, "Lawmakers ask for deeper look into FDA security hack," TheVerge.com, Dec. 9, 2013, http://www.theverge.com/us-world/2013/12/9/5194260/lawmakers-ask-for-deeper-look-into-fda-security-hack, accessed January 13, 2014.

[5] "Fiscal Year 2012 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002," Office of Management and Budget, March 2013, p. 17, http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy12_fisma.pdf, accessed January 13, 2014.

[6] "Fiscal Year 2012 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002," Office of Management and Budget, March 2013, p. 30: Across 22 agencies, "on average the NOC/SOC [Network Operations Center/Security Operations Center] was 63% effective at detecting incidents." http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy12_fisma.pdf, accessed January 13, 2014.

of software which had not been updated in over two years, even though the department had purchased the upgrade.[7]

The President's Order

In February 2012, President Obama unveiled an executive order to protect the nation from debilitating cyberattacks.[8] The president's order addresses the security of computers and networks which run the nation's commercially-owned critical infrastructure. Already, agencies are drawing up plans and working with the private sector to implement the president's directive.

It is appropriate for the White House to envision a federal role in protecting privately-owned infrastructure, particularly when that infrastructure undergirds the nation's economy and society. However, for the country's citizens and businesses to take the government's effort seriously, the federal government should address the immediate danger posed by the insecurity of its own critical networks.

Over more than a decade, the federal government has struggled to implement a mandate to protect its own IT systems from malicious attacks. As we move forward on this national strategy to boost the cybersecurity of our nation's critical infrastructure, we cannot overlook the critical roles played by many government operations, and the dangerous vulnerabilities which persist in their information systems.

Federal Information Security Management Act (FISMA)

Eleven years ago, Congress passed and the White House approved legislation to strengthen the federal government's own computers and networks.[9] The law, known as the Federal Information Security Management Act (FISMA), requires agencies to develop, document, and implement information security programs which meet certain specifications.[10] As Congress again contemplates a major cybersecurity effort, it may be advisable to evaluate how the federal effort has fared. For one thing, FISMA could benefit from reforms of its own. But more importantly, its history can hold clues to the federal government's ability to effectively mandate and enforce cybersecurity standards.

Since 2006, the federal government has spent at least $65 billion on securing its computers and networks, according to an estimate by the Congressional Research Service.[11] The National Institute of Standards and Technology (NIST), the government's official body for

---

[7] Goodin, Dan, "How hackers made minced meat out of the Department of Energy networks," Ars Technica, Dec. 16, 2013, http://arstechnica.com/security/2013/12/how-hackers-made-minced-meat-of-department-of-energy-networks/, accessed January 13, 2014.

[8] "Executive Order – Improving Critical Infrastructure Cybersecurity," White House, February 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity, accessed January 13, 2014.

[9] "Federal Information Security Management Act of 2002," enacted as Title III of the E-Government Act of 2002 (Pub.L. 107-347).

[10] "FISMA: Detailed Overview," NIST, http://csrc.nist.gov/groups/SMA/fisma/overview.html, accessed January 13, 2014.

[11] Congressional Research Service, Memo to HSGAC Minority Staff, "FISMA Spending, Historical Trends," June 6, 2013.

setting cybersecurity standards, has produced thousands of pages of precise guidance on every significant aspect of IT security. And yet agencies — even agencies with responsibilities for critical infrastructure, or vast repositories of sensitive data — continue to leave themselves vulnerable, often by failing to take the most basic steps towards securing their systems and information.

Methodology

This report draws on more than 40 audits and other reviews by agency inspectors general, including mandated annual FISMA audits for nearly a dozen agencies, as well as open-source reporting on cybersecurity and federal agencies. In addition, staff interviewed officials from offices of inspectors general (OIGs) about their cybersecurity work.

Due to the sensitivity of the topic, drafts of this report were shared with relevant OIGs to confirm no sensitive non-public information was inadvertently included which could harm federal cybersecurity efforts.

Department of Homeland Security

In 2010, the Administration tasked the Department of Homeland Security to lead the federal government's efforts to secure its own computers.

Since it was selected to shoulder the profound responsibility of overseeing the security of all unclassified federal networks, one might expect DHS's cyber protections to be a model for other agencies, or that the department had demonstrated an outstanding competence in the field. But a closer look at DHS's efforts to secure its own systems reveals that the department suffers from many of the same shortcomings found at other government agencies.

In August 2010 — just one month after a White House directive gave DHS responsibility for the cybersecurity of all federal government networks — the DHS Inspector General found that the DHS computer security experts who would fulfill that directive had serious cyber vulnerabilities in their own systems. The IG found hundreds of vulnerabilities on the DHS cyber team's systems, including failures to update basic software like Microsoft applications, Adobe Acrobat and Java,[12] the sort of basic security measure just about any American with a computer has performed.

Weaknesses at DHS are not confined to its own cybersecurity office. IT security vulnerabilities exist throughout DHS and its component agencies. Although it has steadily improved its overall cybersecurity performance, DHS is by no means a standard-setter. In fact, in some key areas DHS lags behind many of its agency peers. For instance, in 2013 OMB found DHS rated below the government-wide average for using anti-virus software or other automated detection programs encrypting email, and security awareness training for network users.[13]

In 2013, OMB set a goal for government agencies to send at least 88% of all internet traffic through special secure gateways, known as Trusted Internet Connections (TICs). It set a goal for DHS of 95 percent. The Department's Inspector General reported last November DHS failed to meet either goal. Just 72 percent of DHS internet traffic passed through TICs, the IG stated. It should be noted that DHS is responsible for the administration's efforts to consolidate federal internet traffic through TICs.[14]

---

[12] "DHS Needs to Improve the Security Posture of Its Cybersecurity Program Systems," DHS Office of Inspector General, August 2010, http://www.oig.dhs.gov/assets/Mgmt/OIG_10-111_Aug10.pdf, accessed January 13, 2014.

[13] "Fiscal Year 2012 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002," Office of Management and Budget, March 2013, pp. 31-35, http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy12_fisma.pdf, accessed January 13, 2014.

[14] "OIG-14-09: Evaluation of DHS' Information Security Program for Fiscal Year 2013," DHS Office of Inspector General, November 2013, pp. 3, 15, http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-09_Nov13.pdf, accessed January 13, 2014. DHS has claimed its TIC consolidation numbers have improved since then.

Repeated failure to install software updates and security patches. In 2012, the IG found vulnerabilities arising from missing patches on computers at the National Protection and Programs Directorate (NPPD), which houses the bulk of DHS's cybersecurity efforts; on servers supporting U.S. Secret Service intelligence work; on computers supporting ICE Homeland Security Investigations' Intelligence Fusion Systems, a powerful system allowing agents to query several sensitive databases; and on dozens of servers supporting TSA's Transportation Worker Identification Credential (TWIC) program, which keeps biometric information and credentials for over two million longshoremen, truckers, port employees, mariners and others.[15]

Sensitive databases protected by weak or default passwords.[16] At NPPD, which oversees DHS's cybersecurity programs, the IG found multiple accounts protected by weak passwords. For FEMA's Enterprise Data Warehouse, which handles reports on FEMA's disaster deployment readiness and generates other reports accessing Personally Identifying Information (PII),[17] the IG found accounts protected by "default" passwords, and improperly configured password controls.[18]

Computers controlling physical access to DHS facilities whose antivirus software was out of date. Twelve of the 14 computer servers the IG checked in 2012 had anti-virus definitions most recently updated in August 2011. Several of the servers also lacked patches to critical software components.[19]

Websites with known types of vulnerabilities which could allow a hacker to hijack user accounts, execute malicious scripts, or access sensitive information.[20] Public websites for CBP, FEMA, ICE and even NPPD, home of US-CERT held flaws which could allow unauthorized access, the IG found in 2012. Notably, several vulnerabilities were found in the DHS website "Build Security In" (http://www.buildsecurityin.us-cert.gov).[21] DHS developed the site to encourage software developers "to build security into software in every phase of its development."[22]

Poor physical and information security. Independent auditors physically inspected offices and found passwords written down on desks, sensitive information left exposed, unlocked

---

[15] ITDashboard, "TSA – Transportation Worker Identification Credential (TWIC)," http://www.itdashboard.gov/investment?buscid=170; TWIC Deployment Website, http://www.twicinformation.com/twicinfo/, accessed January 13, 2014; information provided by DHS Office of Inspector General.

[16] Examples of easily-guessed passwords are a person's username or real name, the word "password," the organization's name, or simple keyboard patterns (e.g., "qwerty"), according to the National Institute of Standards and Technology. NIST, "Guide to Enterprise Password Management (Draft), Special Publication 800-118," April 2009, http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-118, accessed January 13, 2014.

[17] "Privacy Impact Assessment for the Operational Data Store (ODS) and Enterprise Data Warehouse (EDW)," June 29, 2012, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_fema_ods_edw_20120629.pdf, accessed January 13, 2014.

[18] Information provided to HSGAC by DHS Office of Inspector General, February 14, 2013.

[19] Information provided to HSGAC by DHS Office of Inspector General, February 14, 2013.

[20] "Evaluation of DHS' Information Security Program for Fiscal Year 2012," DHS Office of Inspector General, October 2012, http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-04_Oct12.pdf, accessed January 13, 2014.

[21] Information provided to HSGAC by DHS Office of Inspector General, February 14, 2013.

[22] "Build Security In," https://buildsecurityin.us-cert.gov/bsi/home.html, accessed January 13, 2014.

laptops, even credit card information. To take just one example, weaknesses found in the office of the Chief Information Officer for ICE included 10 passwords written down, 15 FOUO (For Official Use Only) documents left out, three keys, six unlocked laptops — even two credit cards left out.[23]

[23] "Information Technology Management Letter for the Immigration and Customs Enforcement Component of the FY 2012 Department of Homeland Security Financial Statement Audit," DHS Office of Inspector General, April 2013, http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-60_Apr13.pdf, accessed January 13, 2014.

Nuclear Regulatory Commission

The Nuclear Regulatory Commission (NRC) maintains volumes sensitive, detailed documentation on nuclear facilities. The design and security plans of every nuclear reactor, waste storage facility, and uranium processing facility in the United States; records on every individual licensed to operate or supervise nuclear reactors; and information on the design and process of nuclear material transport all live on the NRC's systems.

Unauthorized disclosure of such sensitive, non-public information "could result in damage to the Nation's critical infrastructure," including nuclear power plants, according to the NRC's Inspector General.[24] Unfortunately, the NRC regularly experiences unauthorized disclosures of sensitive information, or fails to apply adequate measures to protect that data.

Perceived ineptitude of NRC technology experts. There is such "a general lack of confidence" in the NRC's information technology division that NRC offices have effectively gone rogue – by buying and deploying their own computers and networks without the knowledge or involvement of the department's so-called IT experts. Such "shadow IT" systems "can introduce security risks when unsupported hardware and software are not subject to the same security measures that are applied to supported technologies," the NRC Inspector General reported in December 2013. [25]

Sensitive data stored on unsecured shared drive. NRC workers improperly stored and shared sensitive information on an unsecured network drive, according to a 2011 audit. Among the inappropriate data found on the drive: details on nuclear facilities' cybersecurity programs; information on security at fuel cycle facilities; and a Commissioner's passport photo, credit card image, home address and phone number.[26]

Failure to report security breaches. How often does the NRC lose track of or accidentally expose sensitive information to possible release? The NRC can't say, because it has no official process for reporting such breaches. Many involve electronic data stored on the Commission's computers. Of the 95 security lapses which NRC personnel did report between 2005 and 2011, at least a third appear to involve NRC's IT systems.[27]

Inability to keep track of computers. The NRC has had trouble keeping track of its laptop computers, including those which access sensitive information about the nuclear sites the

---

[24] "Semiannual Report to Congress," Nuclear Regulatory Commission Office of the Inspector General, September 30, 2012, http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1415/v25n2/sr1415v25n2.pdf, accessed January 13, 2014.

[25] "Audit of NRC's Information Technology Governance," Nuclear Regulatory Commission Office of the Inspector General, December 9, 2013, pp. i, 8, http://pbadupws.nrc.gov/docs/ML1334/ML13343A244.pdf, accessed January 13, 2014.

[26] "Audit of NRC's Shared "S" Drive," Nuclear Regulatory Commission Office of the Inspector General, July 27, 2011, http://pbadupws.nrc.gov/docs/ML1120/ML112081653.pdf, accessed January 13, 2014.

[27] "Audit of NRC's Protection of Safeguards Information," Nuclear Regulatory Commission Office of the Inspector General, April 16, 2012, http://pbadupws.nrc.gov/docs/ML1210/ML12107A048.pdf, accessed January 13, 2014.

commission regulates.[28] Confusion over laptops' documentation and authorization "could lead to unauthorized use of NRC resources or release of sensitive information," the NRC OIG warned in 2012.[29]

General Sloppiness. Federal guidelines are clear: when an agency identifies a weakness in its IT security, officials must record the problem, find a way to fix it, and assign themselves a deadline for completion. As officials make progress and the weakness is eventually remedied, officials are supposed to update their records. Without that basic system in place, neither the agency nor the administration can tell if vulnerabilities are being addressed.

Yet just about every aspect of that process appears to be broken at the NRC. Problems were identified but never scheduled to be fixed; fixes were scheduled but not completed; fixes were recorded as complete when they were not. In 2012, the IG reported the NRC was "not effective at monitoring the progress of corrective efforts relative to known weaknesses in IT security controls."[30] Last November, a year later, the IG found that nothing had changed, and that the NRC's efforts "are still not effective at monitoring the progress of corrective efforts … and therefore do not provide an accurate measure of security program effectiveness."[31]

[28] "Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act (FISMA) for Fiscal Year 2012," Nuclear Regulatory Commission Office of the Inspector General, November 8, 2012, pp. 5-6, http://pbadupws.nrc.gov/docs/ML1231/ML12313A195.pdf, accessed January 13, 2014.

[29] "Information of Security Risk Evaluation of Region II – Atlanta, GA," Nuclear Regulatory Commission Office of the Inspector General, August 27, 2012, p. 10, http://www.nrc.gov/reading-rm/doc-collections/insp-gen/2012/oig-12-a-17.pdf, accessed January 13, 2014.

[30] "Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act (FISMA) for Fiscal Year 2012," Nuclear Regulatory Commission Office of the Inspector General, November 8, 2012, http://pbadupws.nrc.gov/docs/ML1231/ML12313A195.pdf, accessed January 13, 2014.

[31] "Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act for Fiscal Year 2013," Nuclear Regulatory Commission Office of Inspector General, November 22, 2013, http://pbadupws.nrc.gov/docs/ML1332/ML13326A090.pdf, accessed January 13, 2014.

Internal Revenue Service

The Internal Revenue Service (IRS) collects federal taxes owed by any person or business in the United States, and its computers hold more sensitive data on more Americans than those of perhaps any other federal component. In addition to traditional records on employment, income and identifier information, the IRS reportedly collects a huge volume of personal information on Americans' credit card transactions, eBay activities, Facebook posts and other online behavior.[32]

Unfortunately, the IRS has struggled with the same serious cybersecurity issues for years, and has moved too slowly to correct them.

The IRS' internal watchdog, the Treasury Inspector General for Tax Administration (TIGTA), believes data security is the most serious management challenge facing the IRS.[33] For years, the Government Accountability Office (GAO) has also warned IRS its computers are not safe — that in fact, they are dangerously vulnerable to intrusion and data theft.[34]

Every year since 2008, GAO has identified about 100 cybersecurity weaknesses at the IRS which compromise the agency's computers and data, often repeating weaknesses it cited the previous year.[35] Every year, the IRS claims to fix about half of them, but GAO says even those disappointing numbers aren't right, because IRS doesn't confirm the actions they take actually fix the problems.[36] And every year, GAO returns and finds around 100 problems with IRS' cybersecurity.[37]

Fails to encrypt sensitive data. IRS routinely fails to encrypt its data — converting sensitive data into complex code, making it difficult to read without a key to de-encrypt the

---

[32] Satran, Richard, "IRS High-Tech Tools Track Your Digital Footprints," U.S. News and World Report, April 4, 2013, http://money.usnews.com/money/personal-finance/mutual-funds/articles/2013/04/04/irs-high-tech-tools-track-your-digital-footprints, accessed January 13, 2014.

[33] "Management and Performance Challenges Facing the Internal Revenue Service for Fiscal Year 2014," Treasury Inspector General for Tax Administration, November 8, 2013, http://www.treasury.gov/tigta/management/management_fy2014.pdf, accessed January 13, 2014.

[34] "INFORMATION SECURITY: IRS Has Improved Controls but Needs to Resolve Weaknesses," Government Accountability Office, March 2013, http://www.gao.gov/assets/660/653086.pdf, accessed January 13, 2014; "INFORMATION SECURITY: IRS Needs to Further Enhance Internal Control over Financial Reporting and Taxpayer Data," Government Accountability Office, March 2012, http://www.gao.gov/assets/590/589399.pdf, accessed January 13, 2014; "INFORMATION SECURITY: IRS Needs to Enhance Internal Control over Financial Reporting and Taxpayer Data," Government Accountability Office, March 2011, http://www.gao.gov/assets/320/316569.pdf, accessed January 13, 2014; "INFORMATION SECURITY: IRS Needs to Continue to Address Significant Weaknesses," Government Accountability Office, March 2010, http://gao.gov/assets/310/302087.pdf, accessed January 13, 2014; "INFORMATION SECURITY: Continued Efforts Needed to Address Significant Weaknesses at IRS," Government Accountability Office, January 2009, http://gao.gov/assets/290/284722.pdf, accessed January 13, 2014; "INFORMATION SECURITY: IRS Needs to Address Pervasive Weaknesses," Government Accountability Office, January 2008, http://gao.gov/assets/280/270917.pdf, accessed January 13, 2014.

[35] Ibid.

[36] Ibid.

[37] Ibid.

information — or it encrypts the data so weakly that it can be easily decoded.[38] Since at least 2009, GAO has repeatedly identified instances where IRS did not properly encrypt sensitive data including tax, accounting, and financial information, as well as usernames and passwords. Failing to encrypt or weakly encrypting those data makes it easier for a malicious actor to download, view, and possibly even change taxpayer information and IRS systems.[39]

Lousy user passwords. In March 2013, GAO reported that IRS allowed its employees to use passwords that "could be easily guessed." Examples of easily-guessed passwords are a person's username or real name, the word "password," the agency's name, or simple keyboard patterns (e.g., "qwerty"), according to the National Institute of Standards and Technology.[40] In some cases, IRS users had not changed their passwords in nearly two years.[41] As a result someone might gain unauthorized access to taxpayers' personal information and it "would be virtually undetectable," potentially for years.[42] GAO has cited IRS for allowing old, weak passwords in every one of its reports on IRS' information security for the past six years.[43]

Officials don't properly fix known vulnerabilities. IRS employees monitored its computers by running programs which flagged vulnerabilities in equipment and software, but

[38] "INFORMATION SECURITY: IRS Has Improved Controls but Needs to Resolve Weaknesses," Government Accountability Office, March 2013, p. 10, http://www.gao.gov/assets/660/653086.pdf, accessed January 13, 2014; "INFORMATION SECURITY: IRS Needs to Further Enhance Internal Control over Financial Reporting and Taxpayer Data," Government Accountability Office, March 2012, p. 9, http://www.gao.gov/assets/590/589399.pdf, accessed January 13, 2014; "INFORMATION SECURITY: IRS Needs to Enhance Internal Control over Financial Reporting and Taxpayer Data," Government Accountability Office, March 2011, p. 9, http://www.gao.gov/assets/320/316569.pdf, accessed January 13, 2014; "INFORMATION SECURITY: IRS Needs to Continue to Address Significant Weaknesses," Government Accountability Office, March 2010, p. 9, http://gao.gov/assets/310/302087.pdf, accessed January 13, 2014; "INFORMATION SECURITY: Continued Efforts Needed to Address Significant Weaknesses at IRS," Government Accountability Office, January 2009, p. 11, http://www.gao.gov/assets/290/284722.pdf, accessed January 13, 2014; "INFORMATION SECURITY: IRS Needs to Address Pervasive Weaknesses," Government Accountability Office, January 2008, p. 12, http://www.gao.gov/assets/280/270917.pdf, accessed January 13, 2014.

[39] Ibid.

[40] NIST, "Guide to Enterprise Password Management (Draft), Special Publication 800-118," April 2009, http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf, accessed January 13, 2014.

[41] "INFORMATION SECURITY: IRS Has Improved Controls but Needs to Resolve Weaknesses," Government Accountability Office, pp. 7–8, March 2013, http://www.gao.gov/assets/660/653086.pdf, accessed January 13, 2014.

[42] Ibid.

[43] Ibid; "INFORMATION SECURITY: IRS Needs to Further Enhance Internal Control over Financial Reporting and Taxpayer Data," Government Accountability Office, March 2012, p. 7, http://www.gao.gov/assets/590/589399.pdf, accessed January 13, 2014; "INFORMATION SECURITY: IRS Needs to Enhance Internal Control over Financial Reporting and Taxpayer Data," Government Accountability Office, March 2011, p. 7, http://www.gao.gov/assets/320/316569.pdf, accessed January 13, 2014; "INFORMATION SECURITY: IRS Needs to Continue to Address Significant Weaknesses," Government Accountability Office, March 2010, p. 7, http://gao.gov/assets/310/302087.pdf, accessed January 13, 2014; "INFORMATION SECURITY: Continued Efforts Needed to Address Significant Weaknesses at IRS," Government Accountability Office, January 2009, p. 10, http://www.gao.gov/assets/290/284722.pdf, accessed January 13, 2014; "INFORMATION SECURITY: IRS Needs to Address Pervasive Weaknesses," Government Accountability Office, January 2008, p. 10, http://www.gao.gov/assets/280/270917.pdf, accessed January 13, 2014.

then failed to fix the issues. As a result, scans repeatedly flagged the same vulnerabilities "for two or three consecutive months."[44]

Dangerously slow to install crucial software updates and patches. In March 2012, IRS computers had 7,329 "potential vulnerabilities" because critical software patches had not been installed on computer servers which needed them.[45] At one point in 2011, over a third of all computers at the IRS had software with critical vulnerabilities that were not patched.[46] IRS officials said they expect critical patches to be installed within 72 hours. But TIGTA found it took the IRS 55 days, on average, to get around to installing critical patches.[47] Most recently, in September 2013, TIGTA re-affirmed that the IRS still "has not yet fully implemented a process to ensure timely and secure installation of software patches."[48]

[44] "Federal Information Security Management Act Report for Fiscal Year 2012," Treasury Inspector General for Tax Administration, September 28, 2012, pp. 7-8, http://www.treasury.gov/tigta/auditreports/2012reports/201220114fr.pdf, accessed January 13, 2014.

[45] "Federal Information Security Management Act Report for Fiscal Year 2012," Treasury Inspector General for Tax Administration, September 28, 2012, http://www.treasury.gov/tigta/auditreports/2012reports/201220114fr.pdf, accessed January 13, 2014.

[46] "Federal Information Security Management Act Report for Fiscal Year 2012," Treasury Inspector General for Tax Administration, September 28, 2012, p. 7, http://www.treasury.gov/tigta/auditreports/2012reports/201220114fr.pdf, accessed January 13, 2014.

[47] "An Enterprise Approach Is Needed to Address the Security Risk of Unpatched Computers," Treasury Inspector General for Tax Administration, September 25, 2012, p. 10, http://www.treasury.gov/tigta/auditreports/2012reports/201220112fr.pdf, accessed January 13, 2014.

[48] "Federal Information Security Management Act Report for Fiscal Year 2013," Treasury Inspector General for Tax Administration, September 27, 2013, p. 7, http://www.treasury.gov/tigta/auditreports/2013reports/201320126fr.pdf, accessed January 13, 2014.

Department of Education

The Department of Education holds and manages $948 billion in student loans made to more than 30 million borrowers. The Department's computers hold volumes of information on those borrowers — loan applications, credit checks, repayment records and more.[49]

Given the mammoth store of sensitive information the department keeps, it is disappointing that its Inspector General has said there is little assurance that sensitive data has not been altered or stolen from the computer systems which undergird its lending program.[50]

"[T]he Department's information is vulnerable to attacks that could lead to a loss of confidentiality," the IG concluded. "Also, there is increased risk that unauthorized activities … could reduce the reliability and integrity of Department systems and data."[51]

No review for malicious activity. The Education Department provides remote access to student financial data to Department officials who are off-site or teleworking. Those remote access accounts can be easily compromised by hackers, who use keylogger malware to steal login information from official's computers by secretly recording their keystrokes.

In 2011 and 2012, The Education Department's Federal Student Aid (FSA) office reported 819 compromised accounts. In only 17 percent of those cases did the Department review activity for those accounts to see whether any malicious activity had occurred.[52] Although the financial data is maintained by outside contractors, some of the Department's contracts for those services don't ensure it has access to audit logs for this purpose.[53]

In fact, the Education Department failed to ensure the contractor properly protected borrowers' sensitive personal and financial information; adequately configured their systems

---

[49] U.S. Department of Education, Office of Federal Student Aid, *Annual Report 2012*, p. 2, http://www2.ed.gov/about/reports/annual/2012report/fsa-report.pdf, accessed January 13, 2014.

[50] Inspector General Tighe testimony before the House Oversight and Government Reform Committee, March 5, 2013, pages 10-11, http://cq.com/doc/testimony-4230838#testimony, accessed January 13, 2014.

[51] "The U.S. Department of Education's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2012," Office of Inspector General, Department of Education, November 2012, p. 9, http://www2.ed.gov/about/offices/list/oig/auditreports/fy2013/a11m0003.pdf, accessed January 13, 2014.

[52] "The U.S. Department of Education's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2012," Office of Inspector General, Department of Education, November 2012, p. 10, http://www2.ed.gov/about/offices/list/oig/auditreports/fy2013/a11m0003.pdf, accessed January 13, 2014.

[53] "The U.S. Department of Education's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2012," Office of Inspector General, Department of Education, November 2012, p. 11, http://www2.ed.gov/about/offices/list/oig/auditreports/fy2013/a11m0003.pdf, accessed January 13, 2014.

with security measures; identified and corrected flaws in their IT system; or adequately managed configuration settings and patching updates.[54]

Unsecure networks. Stealing login data wasn't the only way for hackers to potentially compromise the Department's network infrastructure. In 2011, 2012 and 2013, auditors were able to connect a "rogue" computer and other hardware to the Education Department's networks without being noticed. This same access could allow a hacker to drop into the network environment behind the firewalls and other perimeter security.[55]

In June 2013, when its auditors succeeded with this same "rogue" penetration test, they were even able to access sensitive data stored in the department's networked printers "which could be used in a possible social engineering attack." [56]

Vulnerable user accounts. Hundreds of user accounts employed passwords that had not been changed for over 90 days, and many which had not been changed in over a year, the Inspector General found. The Department also failed to deactivate accounts which had been dormant for 90 days. Both are violations of the Department's own policies, meant to protect against unauthorized access by malicious actors, including hackers and ex-employees.[57] Also, while the Department had distributed authentication tokens to many of its employees – which is required by DHS and OMB guidance – fewer than half were activated for use, the OIG found.[58]

---

[54] "Security Controls for Data Protection over the Virtual Data Center (Plano, TX)," Office of Inspector General, Department of Education, September 2010, p. 2, http://www2.ed.gov/about/offices/list/oig/auditreports/fy2010/a11j0006.pdf, accessed January 13, 2014.

[55] "The U.S. Department of Education's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2012," Office of Inspector General, Department of Education, November 2012, p. 8, http://www2.ed.gov/about/offices/list/oig/auditreports/fy2013/a11m0003.pdf, accessed January 13, 2014.

[56] "The U.S. Department of Education's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2013," November 2013, p. 10. http://www2.ed.gov/about/offices/list/oig/auditreports/fy2014/a11n0001.pdf, accessed January 13, 2014.

[57] "The U.S. Department of Education's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2013," November 2013, pp. 12-13, http://www2.ed.gov/about/offices/list/oig/auditreports/fy2014/a11n0001.pdf, accessed January 13, 2014.

[58] "The U.S. Department of Education's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2013," November 2013, p. 24, http://www2.ed.gov/about/offices/list/oig/auditreports/fy2014/a11n0001.pdf, accessed January 13, 2014.

Department of Energy

The many agencies and offices of the sprawling Department of Energy touch nearly every aspect of the nation's energy infrastructure, from generation to transmission and transportation, commercial exchange, research and more. Given how critical its operations are to the national economy and security, one might expect its technology to be more securely protected than most other agencies.

Instead, a close inspection shows the Energy Department's cybersecurity suffers from many of the same basic vulnerabilities and weaknesses found at other federal institutions, which increase the risk that the department's systems could be hacked, and even brought down.[59] Indeed, in January 2013 hackers reportedly compromised 14 servers and 20 workstations, and made off with personal information on hundreds of government and contract employees, and possibly other information.[60] And last July, hackers made off with personal information for 104,000 past and present employees.[61]

Widespread weaknesses at power distribution agency. In October 2012, the Energy IG released an alarming report on cybersecurity weaknesses at the Western Area Power Administration, which markets and delivers wholesale electricity to power millions of homes and businesses through 15 central and western states. "Nearly all" of the 105 computers tested had at least one out-of-date patch; a public-facing server was configured with a default name and password, which "could have allowed an attacker with an Internet connection to obtain unauthorized access to an internal database supporting the electricity scheduling system." What's more, officials at the agency "did not always identify and correct known vulnerabilities." One reason the IG cited: although officials ran vulnerability checks on their IT systems, they ran "less intrusive" scans so as not to slow overall system performance. But those lightweight scans sometimes missed significant weaknesses.[62]

Weak usernames, passwords, and other access controls. The Energy Department's Inspector General found during a 2012 review over a quarter of the sites examined had weak

[59] "Evaluation Report: The Department's Unclassified Cyber Security Program – 2012," Department of Energy Office of the Inspector General, November 2012, pp. 2-3, http://energy.gov/sites/prod/files/IG-0877.pdf, accessed January 13, 2014.

[60] Perlroth, Nicole, "Energy Department Is the Latest Victim of an Online Attack," New York Times, February 4, 2013, http://bits.blogs.nytimes.com/2013/02/04/energy-department-is-the-latest-victim-of-an-online-attack/, accessed January 13, 2014.

[61] Goodin, Dan, "How hackers made minced meat out of the Department of Energy networks," Ars Technica, Dec. 16, 2013, http://arstechnica.com/security/2013/12/how-hackers-made-minced-meat-of-department-of-energy-networks/, accessed January 13, 2014.

[62] "Audit Report: Management of Western Area Power Administration's Cyber Security Program," Department of Energy Office of the Inspector General, October 2012, pp. 1-2, http://energy.gov/sites/prod/files/IG-0873.pdf, accessed January 13, 2014.

access controls. The problems included weak usernames and passwords; accounts with improper access; and a server with insufficient security to prevent it from being remotely controlled.[63]

Failure to apply critical patches and updates to software. In 2013, the IG found that 41 percent of the Department's desktop computers auditors examined were running operating systems or applications which had known vulnerabilities that were not patched, even though the software developers had made patches available.[64] In 2012, the IG's team found 41 network servers running operating systems that were no longer supported by the developer, meaning that even when vulnerabilities were discovered in the system, no patch would be made available.[65]

Vulnerable web applications. Several Department web applications had weak security, increasing the risk a hacker could gain unauthorized access to sensitive systems and obtain information, add or change data, or inject flaws or malicious code, the IG found. The weaknesses included the sorts which are considered the most commonly exploited vulnerabilities for web applications.[66]

Unprotected servers. Eleven servers checked by the OIG last year had no password protections or default/weak passwords, meaning an attacker could gain access to the systems, and could use them to attack other systems on the Department's network. One of the unprotected machines the OIG found was a payroll server, which was configured to allow remote access to anyone, without a username or password.[67]

---

[63] "Evaluation Report: The Department's Unclassified Cyber Security Program – 2012," Department of Energy Office of the Inspector General, November 2012, pp. 2-3, http://energy.gov/sites/prod/files/IG-0877.pdf, accessed January 13, 2014.

[64] "Evaluation Report: The Department of Energy's Unclassified Cyber Security Program – 2013," Department of Energy Office of the Inspector General, October 2013, http://energy.gov/sites/prod/files/2013/11/f4/IG-0897.pdf, accessed January 13, 2014.

[65] "Evaluation Report: The Department's Unclassified Cyber Security Program – 2012," Department of Energy Office of the Inspector General, November 2012, pp. 3-4, http://energy.gov/sites/prod/files/IG-0877.pdf, accessed January 13, 2014.

[66] "Evaluation Report: The Department's Unclassified Cyber Security Program – 2012," Department of Energy Office of the Inspector General, November 2012, pp. 4-5, http://energy.gov/sites/prod/files/IG-0877.pdf, accessed January 13, 2014.

[67] "Evaluation Report: The Department of Energy's Unclassified Cyber Security Program – 2013," Department of Energy Office of the Inspector General, October 2013, http://energy.gov/sites/prod/files/2013/11/f4/IG-0897.pdf, accessed January 13, 2014.

Securities and Exchange Commission

Over the last two decades, financial markets have become increasingly reliant on technology to handle the expanding volume of their business. Today, exchanges like the New York Stock Exchange process millions of trades a day electronically.

In response, the Securities and Exchange Commission (SEC) developed a dedicated team within its Trading and Markets Division to keep an eye on how markets build and manage key trading systems. Among the division's duties is ensuring markets safeguard their systems from hackers and other malicious cyber intruders.

But a 2012 investigation into the team found conduct which did not reflect a concern for security. Team members transmitted sensitive non-public information about major financial institutions using their personal e-mail accounts.[68] They used unencrypted laptops to store sensitive information, in violation of SEC policy — and contravening their own advice to the stock exchanges.[69] Their laptops also lacked antivirus software.[70] The laptops contained "vulnerability assessments and maps and networking diagrams of how to hack into the exchanges," according to one SEC official.[71]

The investigation also found that members of the team took work computers home in order to surf the web, download music and movies, and other personal pursuits.[72] They also appeared to have connected laptops containing sensitive information to unprotected wi-fi networks at public locations like hotels — in at least one reported case, at a convention of computer hackers.[73]

---

[68] "Investigation Into Misuse of Resources and Violations of Information Technology Security Policies Within the Division of Trading and Markets," Securities and Exchange Commission Office of Inspector General, Aug. 30, 2012, http://www.sec-oig.gov/Reports/OOI/2012/OIG-557.pdf, accessed June 10, 2013; Lynch, Sarah N., "U.S. SEC staffers used govn't computers for personal use," November 9, 2012, http://www.reuters.com/article/2012/11/09/sec-cyber-report-idUSL1E8M9CMI20121109, accessed January 13, 2014.

[69] Lynch, Sarah N., "EXCLUSIVE: SEC left computers vulnerable to cyber attacks," Reuters, November 9, 2012.

[70] "Investigation Into Misuse of Resources and Violations of Information Technology Security Policies Within the Division of Trading and Markets," Securities and Exchange Commission Office of Inspector General, Aug. 30, 2012, p.3, http://www.sec-oig.gov/Reports/OOI/2012/OIG-557.pdf, accessed January 13, 2014.

[71] Lynch, Sarah N., "NYSE hires ex-homeland security chief after SEC security lapse," Reuters, November 16, 2012, http://www.reuters.com/article/2012/11/16/sec-cyber-nyse-idUSL1E8MG95K20121116, accessed January 13, 2014.

[72] "Investigation Into Misuse of Resources and Violations of Information Technology Security Policies Within the Division of Trading and Markets," Securities and Exchange Commission Office of Inspector General, Aug. 30, 2012, p.24, http://www.sec-oig.gov/Reports/OOI/2012/OIG-557.pdf, accessed January 13, 2014.

[73] Lynch, Sarah N., "U.S. SEC staffers used govn't computers for personal use," November 9, 2012, http://www.reuters.com/article/2012/11/09/sec-cyber-report-idUSL1E8M9CMI20121109, accessed January 13, 2014.

The investigation also found that while SEC policy prohibited employees from accessing personal e-mail from web-based sites like Gmail, SEC officials in the division arranged to access an internet-connected network which did not block such sites.[74] These employees also brought in their own personal computers and connected them to the SEC's network.[75] And for a period of several months, the team's network had no firewall or intrusion protection software running.[76] All of these practices increased the risk of introducing viruses and other malware to SEC computers, and potentially compromised sensitive data about the cybersecurity of securities exchanges, not to mention the SEC's own protections.[77]

[74] "Investigation Into Misuse of Resources and Violations of Information Technology Security Policies Within the Division of Trading and Markets," Securities and Exchange Commission Office of Inspector General, Aug. 30, 2012, p.31, http://www.sec-oig.gov/Reports/OOI/2012/OIG-557.pdf, accessed January 13, 2014.

[75] "Investigation Into Misuse of Resources and Violations of Information Technology Security Policies Within the Division of Trading and Markets," Securities and Exchange Commission Office of Inspector General, Aug. 30, 2012, p.35, http://www.sec-oig.gov/Reports/OOI/2012/OIG-557.pdf, accessed January 13, 2014.

[76] "Investigation Into Misuse of Resources and Violations of Information Technology Security Policies Within the Division of Trading and Markets," Securities and Exchange Commission Office of Inspector General, Aug. 30, 2012, p.34, http://www.sec-oig.gov/Reports/OOI/2012/OIG-557.pdf, accessed January 13, 2014.

[77] "Investigation Into Misuse of Resources and Violations of Information Technology Security Policies Within the Division of Trading and Markets," Securities and Exchange Commission Office of Inspector General, Aug. 30, 2012, p.30, http://www.sec-oig.gov/Reports/OOI/2012/OIG-557.pdf, accessed January 13, 2014.