

ONE HUNDRED FOURTEENTH CONGRESS  
**Congress of the United States**  
**House of Representatives**  
 COMMITTEE ON ENERGY AND COMMERCE  
 2125 RAYBURN HOUSE OFFICE BUILDING  
 WASHINGTON, DC 20515-6115

Majority (202) 225-2927  
 Minority (202) 225-3641

**MEMORANDUM**

**February 27, 2015**

**To: Subcommittee on Oversight and Investigations Democratic Members and Staff**

**Fr: Committee on Energy and Commerce Democratic Staff**

**Re: Hearing on “Understanding the Cyber Threat and Implications for the 21st Century Economy”**

On Tuesday, March 3, 2015, at 2:00 p.m. in room 2322 of the Rayburn House Office Building, the Subcommittee on Oversight and Investigations will hold a hearing titled “Understanding the Cyber Threat and Implications for the 21st Century Economy.” The majority has indicated that this hearing will provide a broad overview of cybersecurity issues, including the structure of the Internet, current trends and emerging threats, and the future of technology. This is the first in a series of hearings exploring the evolution of cyber threats and the future of cybersecurity.

**I. BACKGROUND**

Cybersecurity involves the protection of information and communications technology (ICT) systems and their content.<sup>1</sup> In the past decade, experts and policy makers have expressed concerns with the increasing frequency and severity of cyberattacks in both the private sector and on government entities. Cyberattack risks can be defined by threats (who is attacking), vulnerabilities (how they are attacking), and impacts (what the attack does).

There are five categories of people who generally perform cyberattacks: (1) criminals seeking monetary gain; (2) spies seeking classified or proprietary information; (3) nation-states seeking information in support of a country’s strategic objectives; (4) “hacktivists” performing cyberattacks for non-monetary reasons; and (5) “cyberterrorists” who are using the internet to cause or assist terrorist acts.

Attackers seek to identify weaknesses in a system and infiltrate at particular points of

---

<sup>1</sup> Congressional Research Service, *Cybersecurity Issues and Challenges: In Brief* (Jan. 29, 2015) (online at [www.crs.gov/pdfloader/R43831](http://www.crs.gov/pdfloader/R43831)).

vulnerability. They can use insiders to gain access to the system, or they can target supply chain vulnerabilities and install malicious hardware or software. Attackers can also exploit what experts refer to as “zero-day” vulnerabilities. Zero-day vulnerabilities are coding weaknesses unknown to a software manufacturer or which have no established fix, but are known to hackers.

Certain physical infrastructure—such as pipelines—may be vulnerable to cyber-intrusions because of its reliance on supervisory control and data acquisition (SCADA) systems.<sup>2</sup> SCADA systems are software-based industrial control systems used to control and monitor a host of industrial functions including power grids, pipelines, railways, and sewer plants. Depending upon the configuration of a particular pipeline, for example, a sophisticated cyberattack could potentially disrupt or damage equipment and release hazardous commodities into the environment.<sup>3</sup>

In the past several years, there have been a number of high-profile cyberattacks which have targeted both private-sector and government systems:

- In December 2013, Target learned of a breach into their system and found that customer names, mailing addresses, email addresses, phone numbers, and credit and debit card information were taken. Up to 70 million individuals may have been affected, including approximately 40 million credit and debit card accounts. Hackers were able to obtain the information by installing malware on Target’s security and payment systems.<sup>4</sup> Target offered one year of free credit monitoring to all customers who shopped in U.S. stores.<sup>5</sup>
- In August 2014, JPMorgan Chase disclosed that a cyberattack on its systems compromised the information of 76 million households and seven million small businesses. The attack was part of a broader attack by Russian hackers that infiltrated more than 420,000 websites.<sup>6</sup>
- Beginning in September 2014, Home Depot learned of a cyberattack on their payment systems, resulting in information for 56 million credit and debit cards being taken. In the course of their investigation, Home Depot also found that 53 million email addresses were also stolen. Hackers were able to obtain the

---

<sup>2</sup> Congressional Research Service, *Pipeline Cybersecurity: Federal Policy* (Aug. 16, 2012) (online at [www.crs.gov/pages/Reports.aspx?PRODCODE=R42660&Source=search](http://www.crs.gov/pages/Reports.aspx?PRODCODE=R42660&Source=search)).

<sup>3</sup> *Id.*

<sup>4</sup> Bloomberg, *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It* (Mar. 31, 2014) (online at [www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data](http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data)).

<sup>5</sup> Target, *data breach FAQ* (online at [corporate.target.com/about/shopping-experience/payment-card-issue-FAQ#q5888](http://corporate.target.com/about/shopping-experience/payment-card-issue-FAQ#q5888)).

<sup>6</sup> New York Times, *Neglected Server Provided Entry for JPMorgan Hackers* (Dec. 22, 2014) (online at [dealbook.nytimes.com/2014/12/22/entry-point-of-jpmorgan-data-breach-is-identified/](http://dealbook.nytimes.com/2014/12/22/entry-point-of-jpmorgan-data-breach-is-identified/)).

information by installing malware on Home Depot's self-checkout registers. Home Depot has offered credit monitoring, identity monitoring, and identity theft insurance policies to its customers.<sup>7</sup>

- In November 2014, Sony Pictures revealed a data breach where hackers posted threatening messages on company computers, resulting in the shutdown of email communications and computers. The leaked files involved personal data on 47,000 individuals, including celebrities and Sony employees, and 33,000 company documents that included salary information, contracts, and termination information. Sony offered one year of fraud protection to affected individuals.<sup>8</sup>
- In January 2015, Anthem announced that it had discovered a cyberattack on its IT system. Anthem found that the leaked records – for nearly 80 million customers – included social security numbers, employment information, and income data. Anthem has stated that they do not believe the breach captured medical information or credit card information. Anthem is offering two years of identity protection services to its customers.<sup>9</sup>

The federal government has also been the target of an increasing number of cyberattacks. For example, according to the most recent GAO High Risk report, federal agencies have reported over a 1000-percent increase in the number of information-security incidents in the last eight years, rising from 5,503 incidents in FY2006 to 67,168 incidents in FY2014.

As one example of a federal attack, in November 2014, National Oceanic and Atmospheric Administration (NOAA) officials reported that hackers breached the federal weather network, resulting in the agency needing to seal off data vital to disaster planning, aviation, and shipping.<sup>10</sup>

There have also been several reported breaches of federal agencies that may have

---

<sup>7</sup> USA Today, *Home Depot hackers used vendor log-on to steal data, e-mails* (Nov. 7, 2014) (online at [www.usatoday.com/story/money/business/2014/11/06/home-depot-hackers-stolen-data/18613167/](http://www.usatoday.com/story/money/business/2014/11/06/home-depot-hackers-stolen-data/18613167/)).

<sup>8</sup> Wall Street Journal, *Sony Hack Exposed Personal Data of Hollywood Stars* (Dec. 5, 2014) (online at [www.wsj.com/articles/sony-pictures-hack-reveals-more-data-than-previously-believed-1417734425](http://www.wsj.com/articles/sony-pictures-hack-reveals-more-data-than-previously-believed-1417734425)).

<sup>9</sup> Reuters, *Anthem says at least 8.8 million non-customers could be victims in data hack* (Feb. 25, 2015) (online at [www.reuters.com/article/2015/02/24/us-anthem-cybersecurity-idUSKBN0LS2CS20150224](http://www.reuters.com/article/2015/02/24/us-anthem-cybersecurity-idUSKBN0LS2CS20150224)) and Anthem, *Frequently Asked Questions* (online at [www.anthemfacts.com/faq](http://www.anthemfacts.com/faq)).

<sup>10</sup> Washington Post, *Chinese hack U.S. weather systems, satellite network* (Nov. 12, 2014) (online at [www.washingtonpost.com/local/chinese-hack-us-weather-systems-satellite-network/2014/11/12/bef1206a-68e9-11e4-b053-65cea7903f2e\\_story.html](http://www.washingtonpost.com/local/chinese-hack-us-weather-systems-satellite-network/2014/11/12/bef1206a-68e9-11e4-b053-65cea7903f2e_story.html)).

compromised personally-identifiable information (PII).<sup>11</sup> For example, in May of 2012, PII hackers accessed data on 123,000 participants from the Federal Thrift Savings Plan.<sup>12</sup> In July of 2013, PII data on 140,000 individuals was removed from the Department of Energy, which included birthdates, bank accounts, and social security numbers.<sup>13</sup>

## II. ROLE OF THE FEDERAL GOVERNMENT

The principal law concerning the federal government's information security program is the 2002 Federal Information Security Management Act (FISMA), also known as Title II of the E-Government Act of 2002 (P.L. 107-347). This law requires federal agencies to provide information security protections for agency information systems.<sup>14</sup> The law was amended in 2014 to clarify and strengthen information security roles and responsibilities of the Office of Management and Budget (OMB), the Department of Homeland Security (DHS), and other federal agencies. The law also expanded reporting of security incidents and data breaches.

FISMA makes OMB chiefly responsible for overseeing federal information-security policy, evaluating agency security programs, and implementing new cybersecurity standards developed by the National Institute of Standards and Technology (NIST). FISMA also requires agencies to inventory and continuously evaluate their respective computer systems for weaknesses and vulnerabilities and provide mitigation strategies if risks are found. Under FISMA, each agency must designate an information-security officer (often, a chief information officer) to implement a host of monitoring and protection responsibilities. These responsibilities include training of security personnel and developing procedures for handling security incidents should they occur. Finally, federal agencies must also develop performance plans and undertake annual evaluations of their cybersecurity programs (which they provide to Congress). Importantly, FISMA requirements also apply to contractors who run information systems on behalf of an agency.<sup>15</sup>

A number of executive branch departments and agencies are entrusted with federal government cybersecurity responsibilities. While OMB, in coordination with DHS, is responsible for overseeing the implementation of FISMA, the Department of Defense is

---

<sup>11</sup> Government Accountability Office, *Ensuring the Security of Federal Information Systems and Cyber Critical Infrastructure and Protecting the Privacy of Personally Identifiable Information* (Feb. 11, 2015) (online at [www.gao.gov/highrisk/protecting\\_the\\_federal\\_government\\_information\\_systems/why\\_did\\_study#t=1](http://www.gao.gov/highrisk/protecting_the_federal_government_information_systems/why_did_study#t=1)).

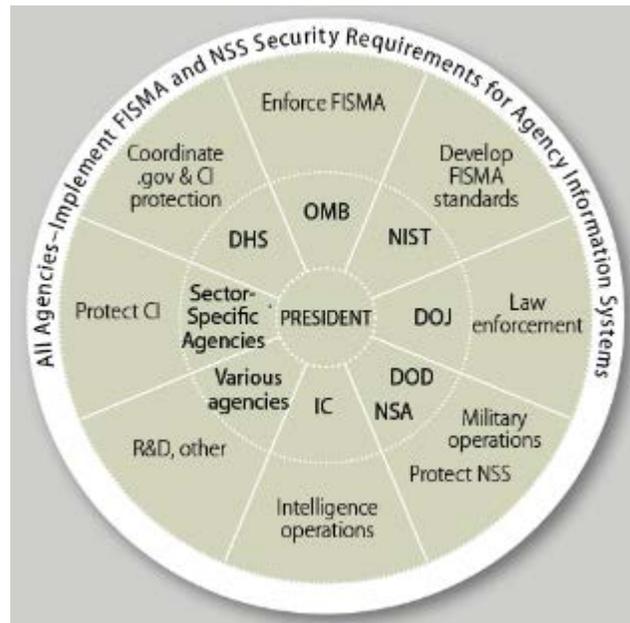
<sup>12</sup> Government Accountability Office: *Information Security: Federal Agencies Need to Enhance Responses to Data Breaches* (Apr. 2, 2014) (online at <http://gao.gov/assets/670/662227.pdf>).

<sup>13</sup> *Id.*

<sup>14</sup> Federal Information Security Management Act of 2002; 44 U.S.C. § 3543.

<sup>15</sup> Congressional Research Service, *Cyber Security: FISMA Reform* (Dec. 15, 2014) (online at [www.crs.gov/pages/Insights.aspx?PRODCODE=IN10186](http://www.crs.gov/pages/Insights.aspx?PRODCODE=IN10186)).

principally responsible for military cyber protection. DHS currently has operational responsibility for protection of federal civilian systems and is the lead agency coordinating federal efforts assisting the private sector in protecting critical infrastructure assets under their control. The Department of Justice (DOJ) is the lead federal agency for enforcement of relevant laws.<sup>16</sup>



Source: *Congressional Research Service*<sup>17</sup>

The Government Accountability Office (GAO) and inspector general reports have identified considerable challenges in designing and implementing critical infrastructure programs and detecting, responding to, and mitigating cyber incidents.<sup>18</sup> DHS has made some progress in coordinating the federal response to cyber incidents, but it continues to face challenges in sharing information among federal agencies and private entities.

On February 12, 2013, President Obama issued Executive Order 13636 on improving critical infrastructure cybersecurity.<sup>19</sup> It directed NIST to work with stakeholders to develop a

<sup>16</sup> Congressional Research Service, *Cybersecurity Issues and Challenges* (Jan. 21, 2015) (online at [www.crs.gov/products/if/pdf/IF10001.pdf?Source=search](http://www.crs.gov/products/if/pdf/IF10001.pdf?Source=search))

<sup>17</sup> *Id.*

<sup>18</sup> Government Accountability Office, *CYBERSECURITY – National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented* (Feb. 2013) (online at [www.gao.gov/assets/660/652170.pdf](http://www.gao.gov/assets/660/652170.pdf)).

<sup>19</sup> Executive Order 13636 – Improving Critical Infrastructure Cybersecurity (Feb. 12, 2013).

voluntary framework for reducing cyber risks to critical infrastructure. In February 2014, NIST released its framework – developed by both industry and government – for standards, guidelines, and practices to manage cybersecurity-related risk.

In February 2015, the White House convened a cybersecurity summit to hear from both government and industry on best practices and security standards and discuss how to improve information sharing and encourage the adoption of more secure payment technologies.<sup>20</sup> The Obama Administration also recently announced the creation of the Cyber Threat Intelligence Integration Center to provide intelligence analysis on cyber threats. It has also recently proposed new legislation in several key areas related to cyber security.<sup>21</sup>

The GAO’s High Risk List has identified the security of federal cyber assets as an area of concern in 1997. In 2015, GAO added the security of personally identifiable information (PII) to the list. In its most recent assessment, GAO recognized the leadership commitment by the White House and DHS to improve cybersecurity. Nonetheless, GAO still found that significant progress is needed at key agencies in this area.

### **III. WITNESSES**

**Herbert Lin, Ph.D.**

Senior Research Scholar for Cyber Policy and Security, Center for International Security and Cooperation  
Senior Fellow, Hoover Institution  
Stanford University

**Richard Bejtlich**

Chief Security Strategist  
FireEye, Inc.

**Greg Shannon, Ph.D.**

Chief Scientist  
CERT Program, the Software Engineering Institute  
Carnegie Mellon University

---

<sup>20</sup> The White House, *Summit on Cybersecurity and Consumer Protection* (Feb. 13, 2015) (online at [www.whitehouse.gov/issues/foreign-policy/cybersecurity/summit](http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/summit)).

<sup>21</sup> The White House, *FACT SHEET: Cyber Threat Intelligence Integration Center* (Feb. 25, 2015).