**U.S. HOUSE OF REPRESENTATIVES**
**COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY**
**SUBCOMMITTEES ON RESEARCH & TECHNOLOGY AND OVERSIGHT**

***Cybersecurity: What the Federal Government Can Learn from the Private Sector***

**Friday, January 8, 2016**
**9:00 a.m. – 11:00 a.m.**
**2318 Rayburn House Office Building**

## Purpose

On Friday, January 8, 2016, the Research & Technology and Oversight Subcommittees will hold a joint hearing to discuss various industry best practices relative to cybersecurity, share lessons learned from the private sector, inform on how innovative private sector security practices can be applied to government agencies, particularly in the wake of data breaches at the Office of Personnel Management (OPM), address the effectiveness of voluntary federal standards for cybersecurity, and discuss implementation of new cyber information sharing legislation. The Science, Space, and Technology Committee previously held a hearing on July 8, 2015 titled, *Is the OPM Data Breach the Tip of the Iceberg?* [1] The Committee's jurisdiction includes the National Institute of Standards and Technology (NIST), which develops cybersecurity standards and guidelines,[2] the Department of Homeland Security's Science and Technology Directorate (DHS S&T) and research and development related to cybersecurity at the National Science Foundation (NSF).

## Witnesses

- **Mr. John B. Wood**, Chief Executive Officer and Chairman, Telos Corporation
- **Dr. Martin Casado**, Senior Vice President and General Manager, Networking and Security Business Unit, VMWare
- **Mr. Ken Schneider**, Vice President of Technology Strategy, Symantec Corporation
- **Mr. Larry Clinton**, President and Chief Executive Officer, Internet Security Alliance

## Background

On June 4, 2015, OPM announced that it had identified a cyber-breach affecting personnel data for approximately 4 million current and former federal employees, including

[1] Hearing information available at: http://science.house.gov/hearing/subcommittee-research-and-technology-and-subcommittee-oversight-hearing-opm-data-breach-tip.

[2] As authorized by the Federal Information Security Management Act (FISMA) of 2002, enacted as Title III of the E-Government Act (Public Law 107-347) in December 2002, available at: http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf. NIST's responsibilities for cybersecurity were last updated in the Cybersecurity Enhancement Act of 2014 (Public Law 113-274) available at: http://www.gpo.gov/fdsys/pkg/PLAW-113publ274/pdf/PLAW-113publ274.pdf, and Federal Information Security Modernization Act (P.L. 113-283) available at: http://www.gpo.gov/fdsys/pkg/PLAW-113publ283/pdf/PLAW-113publ283.pdf.

personally identifiable information (PII).[3] Later that month, OPM reported a separate cyber incident targeting its databases housing background investigation records, and announced on July 9th that an investigation concluded that the information of an additional 19.7 million individuals that applied for a background investigation had been stolen. The combined breaches are estimated to have compromised the sensitive information of 21.5 million individuals.[4]

On November 10, 2015, the OPM Office of Inspector General (OIG) released a FY 2015 audit report for the agency that continued to find an "overall lack of compliance that seems to permeate the agency's IT security program."[5] The audit found that the OPM has up to 23 systems that have not been subject to a thorough security controls assessment. The report states: "Combined with the inadequacy and non-compliance of OPM's continuous monitoring program, we are very concerned that the agency's systems will not be protected against another attack."[6]

The OPM breaches highlight the growing challenges of cybersecurity for both the public and private sector, as the number of cyber threats to both has grown exponentially in recent years. According to the U.S. Government Accountability Office (GAO), the number of information security incidents reported by federal agencies to US-CERT (the U.S. Computer Emergency Readiness Team, part of the Department of Homeland Security) increased from 5,503 in fiscal year 2006 to 67,168 in fiscal year 2014 – an increase of over 1000 percent.[7]

A 2014 survey of private companies found that the number of detected incidents rose to 42.8 million, a 48% increase over 2013. The survey also found that the total financial losses attributed to security compromises increased 34% over 2013.[8] The impact to individual Americans grows too, as an estimated 12.7 million Americans experienced some sort of financial identity theft in 2014, costing $16 billion in financial losses.[9] In 2014 and 2015, cyber-attacks on Target, eBay, Home Depot, J.P. Morgan-Chase, Sony Pictures, and Anthem Health Insurance were only a few of the many publicly disclosed breaches.[10] The data breach of Anthem alone exposed the social security numbers of nearly 80 million Americans.

---

[3] OPM Press Release, "OPM to Notify Employees of Cybersecurity Incident," June 4, 2015. Available at: https://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident.

[4] OPM Press Release, "OPM Announces Steps to Protect Federal Workers and Others from Cyber Threats," July 9, 2015. Available at: https://www.opm.gov/news/releases/2015/07/opm-announces-steps-to-protect-federal-workers-and-others-from-cyber-threats.

[5] OPM FISMA FY 2015 Audit Report. Available at: https://www.opm.gov/our-inspector-general/reports/2015/federal-information-security-modernization-act-audit-fy-2015-final-audit-report-4a-ci-00-15-011.pdf.

[6] Ibid.

[7] *Actions Needed to Address Challenges Facing Federal Systems*, GAO-15-573T, April 22, 2015. Available at: http://www.gao.gov/products/GAO-15-573T.

[8] The Global State of Information Security Survey 2015. Available at: http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml.

[9] Herb Weisbaum, "Nearly 13 Million Americans Victimized by ID Thieves in 2014," NBCNEWS, March 3, 2015. Available at: http://www.nbcnews.com/business/consumer/nearly-13-million-americans-victimized-id-thieves-2014-n316266.

[10] 2014: A Year of Mega Breaches, Ponemon Institute, 1, (January 2015). Available at: http://www.ponemon.org/local/upload/file/2014%20The%20Year%20of%20the%20Mega%20Breach%20FINAL3.pdf.

*Federal Cybersecurity Laws and Regulations*

The federal role in cybersecurity involves both security for federal systems and assisting in protecting nonfederal systems. More than 50 federal statutes address various aspects of cybersecurity. These include:

*Federal Information Security Management Act*

The cybersecurity of federal systems is governed by the Federal Information Security Management Act, which was last updated by the Federal Information Security Modernization Act (P.L. 113-283) in December 2014. FISMA created a security framework for federal information systems, with an emphasis on risk management, and gave specific responsibilities to the Office of Management and Budget (OMB), National Institutes of Standards and Technology (NIST), and the heads, chief information officers (CIOs), chief information security officers (CISOs), and inspectors general (IGs) of federal agencies.[11]

FISMA makes OMB responsible for overseeing federal information-security policy, evaluating agency programs, and promulgating cybersecurity standards developed by NIST. Each agency must designate an information-security officer, with responsibilities including agency-wide programs, policies, and procedures, training of security and other personnel, processes for remedial action to address deficiencies, and procedures for handling security incidents and ensuring continuity of operations. Agencies must also develop performance plans, conduct independent annual evaluations of their cybersecurity programs and practices, and provide annual reports on compliance and effectiveness to Congress. FISMA requirements also apply to contractors who run information systems on behalf of an agency.[12]

*Cybersecurity Enhancement Act of 2014*

In December 2014, the *Cybersecurity Enhancement Act of 2014* (P.L. 113-274) passed the House and Senate and was signed into law. The law strengthens the efforts of NSF and NIST in the areas of cybersecurity technical standards and cybersecurity awareness, education, and workforce development. P.L. 113-274 coordinates research and related activities conducted across federal agencies to better address evolving cyber threats.

In December 2015, pursuant to Section 502 of the law, NIST developed and transmitted to Congress a plan ensuring federal coordination of international technical standards related to information system security. The plan "lays out the objectives and recommendations for enhancing the U.S. government's coordination and participation in the development and use of international standards for cybersecurity. The plan outlines four U.S. government strategic objectives for the development and use of international standards for cybersecurity: enhancing national and economic security and public safety; ensuring standards and assessment tools for

[11] *Information Security: Weaknesses Continue Amid New Federal Efforts to Implement Requirements*, GAO-12-137, October 2011, http://www.gao.gov/new.items/d12137.pdf.
[12] *Cybersecurity: FISMA Reform*, CRS Insights, December 15, 2014.

the U.S. government are technically sound; facilitating international trade; and promoting innovation and competitiveness."[13]

*Cybersecurity Act of 2015*

In December 2015, the Consolidated Appropriations Act (P.L. 114-57) included the *Cybersecurity Act of 2015*. The new law encourages private companies to voluntarily share information about cyber threats with each other as well as the federal government. The Act directs the federal government to create a process for sharing both classified and unclassified cyber threat indicators and defensive measures with the private sector, as well as information relating to certain cybersecurity threats and best practices. Firms that participate in the information sharing will receive some liability protection.[14]

*Executive Order 13636 on Improving Critical Infrastructure and Framework for Improving Critical Infrastructure Cybersecurity*

In February 2013, President Obama issued an executive order (EO) on cybersecurity for critical infrastructure.[15] Among other provisions, the EO encouraged information sharing between public and private sectors and directed NIST to lead the development of a framework to reduce cyber risks to critical infrastructure. NIST was instructed to work with industry to identify existing voluntary consensus standards and industry best practices to incorporate into the framework.

In February 2014, NIST released the *Framework for Improving Critical Infrastructure Cybersecurity* (Framework) in response to the EO. NIST worked in collaboration with industry stakeholders to establish a three-pronged framework that includes a Core, Profile, and Implementation Tiers. "The Framework enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure."[16]

P.L. 113-274 called for GAO to review aspects of the Framework, and in December 2015, GAO issued a report titled, "Critical Infrastructure Protection: Measures Needed to Assess Agencies' Promotion of the Cybersecurity Framework." The report determines "the extent to which (1) NIST facilitated the development of voluntary cybersecurity standards and procedures and (2) federal agencies promoted these standards and procedures."[17]

---

[13] Letter from Dr. Willie E. May, NIST Director, to Chairman Lamar Smith, December 21, 2015.

[14] "President Obama Signs Cybersecurity Act of 2015 to Encourage Cybersecurity Information Sharing," National Law Review. Available at: http://www.natlawreview.com/article/president-obama-signs-cybersecurity-act-2015-to-encourage-cybersecurity-information.

[15] White House Press Release, "Executive Order – Improving Critical Infrastructure Cybersecurity," February 12, 2013. Available at: http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[16] "Framework for Improving Critical Infrastructure Cybersecurity," February 12, 2014. Available at: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[17] *Critical Infrastructure Protection: Measures Needed to Assess Agencies' Promotion of the Cybersecurity Framework*, GAO-16-152, December 17, 2015. Available at: http://www.gao.gov/products/GAO-16-152.