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

Is the OPM Data Breach the Tip of the Iceberg?

Wednesday, July 8 2015
2:00 p.m. – 4:00 p.m.
2318 Rayburn House Office Building

Purpose

On Wednesday, July 8, 2015, the Research and Technology Subcommittee and Oversight Subcommittees will hold a joint hearing to examine recent data breaches at the Office of Personnel Management (OPM), discuss the implications of this breach for former and current employees as well as to the government, and identify the ongoing challenges for protecting personal and sensitive data government-wide from future cyber-attacks. The hearing will also review agency compliance with federal information security guidelines and standards required by the *Federal Information Security Management Act* (FISMA).[1] The Committee's jurisdiction includes the National Institute of Standards and Technology (NIST) who is responsible for key security standards and guidelines to support the implementation of and compliance with FISMA, 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. Michael R. Esser,** Assistant Inspector General for Audits, Office of Personnel Management
- **Mr. David Snell**, Director, Federal Benefits Service Department, National Active and Retired Federal Employees Association
- **Dr. Charles Romine**, Director, Information Technology Laboratory, National Institute of Standards and Technology
- **Mr. Gregory Wilshusen,** Director, Information Security Issues, U.S. Government Accountability Office

Background

On June 4th, 2015 OPM announced that it had identified a cybersecurity breach affecting personnel data for approximately 4 million current and former federal employees, including personally identifiable information (PII).[2] As the investigation into the initial intrusion proceeded, the Interagency Response Team shared with relevant agencies that there was a high degree of confidence that OPM computer systems containing information on background investigations of current, former, and prospective Federal government employees, had been

[1] Federal Information Security Management Act of 2002 (Public Law 107-347), updated by the Federal Information Security Modernization Act of 2014 (Public Law 113-283).
[2] https://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident/

hacked. Early news reports, citing Federal Bureau of Investigation (FBI) sources, estimate that sensitive, personal information of 18 million people have been hacked by these computer breaches.[3] OPM is expected to provide an update on the extent of the second data breach this week.

OPM Investigation and Response

OPM discovered the first breach in April 2015, during the installation of new intrusion software. According to reports, in December 2014, intruders used a "zero-day" exploit — a previously unknown cyber-tool — to access information including "employees' Social Security numbers, job assignments, performance ratings and training information.[4] In testimony before the Senate Appropriations Financial Services and General Government Subcommittee, OPM Director Katherine Archuleta also testified that the intruders in the attack obtained a compromised user credential from a government contractor to help access the system.[5]

Since both incidents were discovered last April, OPM has partnered with the U.S. Department of Homeland Security's Computer Emergency Readiness Team (US-CERT), and the Federal Bureau of Investigation (FBI) to investigate and determine the full impact to federal personnel. Federal officials continue to investigate the source of the attack and assist with remediation efforts.[6] Although officials have not publicly identified the perpetrators, the Director of National Intelligence James Clapper called China a "leading suspect."[7]

OPM is in the process of sending notifications by mail and email to individuals whose information was compromised in the first breach. OPM signed a $21 million contract with the Winvale group and CSID to offer 18 months of credit monitoring and identity theft insurance.[8] Federal employees have since reported long wait times for assistance as well as "phishing campaigns masquerading as emails" from OPM and CSID.[9]

On June 29th, OPM announced the temporary suspension of the Electronic Questionnaires for Investigations Processing (E-QIP) system, a web-based platform used by federal employees to submit security background investigation forms with personal information, until more security measures are implemented. [10] OPM says that they are continuing to work with DHS and the FBI to determine the number of people affected by the second intrusion, and will begin making notifications to affected individuals in July.[11]

[3] http://www.cnn.com/2015/06/22/politics/opm-hack-18-milliion/index.html

[4] https://www.washingtonpost.com/world/national-security/chinese-hackers-breach-federal-governments-personnel-office/2015/06/04/889c0e52-0af7-11e5-95fd-d580f1c5d44e_story.html

[5] http://www.usatoday.com/story/news/politics/2015/06/27/opm-hack-questions-and-answers/29333211/

[6] http://www.opm.gov/news/latest-news/announcements/frequently-asked-questions/

[7] http://www.cnn.com/2015/06/25/politics/james-clapper-china-opm-hacking/

[8] http://www.washingtonpost.com/blogs/federal-eye/wp/2015/06/22/looking-for-help-after-the-federal-employee-hack-prepare-to-spend-a-few-hours-on-hold/

[9] http://www.nextgov.com/cybersecurity/2015/07/dhs-alerts-public-opm-related-phishing-scams/116794/

[10] https://www.opm.gov/news/releases/2015/06/opm-notifies-agencies-of-temporary-suspension-of-e-qip-system/

[11] http://www.washingtonpost.com/blogs/federal-eye/wp/2015/07/02/opm-plans-to-release-more-information-about-data-breach/

OPM Office of Inspector General (OIG) Audits

The OPM OIG has noted that "OPM has a history of struggling to comply with FISMA requirements." FISMA requires OIGs to perform annual audits of their agencies' IT security programs and practices. In 2007, the OPM OIG first identified an IT material weakness at OPM – a severe control deficiency that prohibits the organization from adequately protecting its data. Since that time the OPM OIG has continued to identify major security gaps in OPM's information systems. In 2014, the OPM OIG noted improvements, and changed the classification to a "significant deficiency, which is less serious than a material weakness." However the 2014 report continued to make 29 audit recommendations to OPM to improve technical security controls.[12]

History of Government Data Breaches

The number of cyber threats to both government and private sector information systems 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 increased from 5,503 in fiscal year 2006 to 67,168 in fiscal year 2014 – an increase of over 1000 percent.[13] According to GAO, some recent examples of federal information system breaches include:

- In April 2015, the Department of Veterans Affairs (VA) Office of Inspector General reported that two VA contractors improperly accessed the VA network from foreign countries using personally owned equipment.
- In September 2014, a cyber-intrusion into the United States Postal Service's information systems may have compromised PII for more than 800,000 employees.
- In 2011, according to a media report, the Deputy Secretary of Defense acknowledged a significant cyber-attack in which a large number of files were taken by foreign intruders from a defense contractor. The deputy secretary was quoted as saying "it is a significant concern that over the past decade terabytes of data have been extracted by foreign intruders from corporate networks of defense companies" and that some of the data concerned "our most sensitive systems."[14]

In fiscal year 2014, the federal government spent more than $81 billion on information technology, and "Federal agencies spend a significant part of their annual IT funding on cybersecurity, which currently constitutes more than one in every eight dollars of agency IT budgets."[15]

[12] Statement of Michael R. Esser, Assistant Inspector General for Audits, Committee on Oversight and Government Reform, U.S. House of Representatives, June 16, 2015.

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

[14] http://www.defense.gov/news/newsarticle.aspx?id=64686

[15] http://www.fas.org/sgp/crs/misc/R43831.pdf

A major consequence of a data breach is identity theft, whether the information is used to make purchases, obtain medical care or commit tax fraud. An estimated 12.7 million Americans experienced some sort of financial identity theft in 2014, costing $16 billion in financial losses. Many more Americans are at risk of identity theft, after numerous private and public sector breaches. The 2014 data breach of Anthem Health Insurance alone exposed the social security numbers of nearly 80 million Americans.[16] However, Cyber breaches to federal systems have wide-ranging consequences beyond identity theft, including the ability to adversely affect national security, damage public health and safety, and lead to inappropriate access to other sensitive personal information.

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.

The cybersecurity of federal systems is governed by FISMA, which was 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.[17]

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.[18]

In December 2014, *The Cybersecurity Enhancement Act of 2015* (P.L. 113-270) passed the House and Senate and was signed into law. The new law strengthens the efforts of the National Science Foundation (NSF) and NIST in the areas of cybersecurity technical standards and cybersecurity awareness, education, and workforce development. P.L. 113-270 coordinates research and related activities conducted across the Federal agencies to better address evolving cyber threats.

[16] http://www.nbcnews.com/business/consumer/nearly-13-million-americans-victimized-id-thieves-2014-n316266

[17] *Information Security: Weaknesses Continue Amid New Federal Efforts to Implement Requirements*, GAO-12-137, October 2011, http://www.gao.gov/new.items/d12137.pdf

[18] *Cybersecurity: FISMA Reform*, CRS Insights, December 15, 2014.