Cyber Intrusion into U.S. Office of Personnel Management: In Brief

Kristin Finklea, Coordinator
Specialist in Domestic Security

Michelle D. Christensen
Analyst in Government Organization and Management

Eric A. Fischer
Senior Specialist in Science and Technology

Susan V. Lawrence
Specialist in Asian Affairs

Catherine A. Theohary
Specialist in National Security Policy and Information Operations

July 17, 2015

Congressional Research Service
7-5700
www.crs.gov
R44111

CRS REPORT
Prepared for Members and
Committees of Congress

c11173008

Summary

On June 4, 2015, the U.S. Office of Personnel Management (OPM) revealed that a cyber intrusion had impacted its information technology systems and data, potentially compromising the personal information of about 4.2 million former and current federal employees. Later that month, OPM reported a separate cyber incident targeting OPM's databases housing background investigation records. This breach is estimated to have compromised sensitive information of 21.5 million individuals.

Amid criticisms of how the agency managed its response to the intrusions and secured its information systems, Katherine Archuleta has stepped down as the director of OPM, and Beth Cobert has taken on the role of acting director. In addition, OPM's Electronic Questionnaires for Investigations Processing (e-QIP) application, the system designed to help process forms used in conducting background investigations, has been taken offline for security improvements.

Officials are still investigating the actors behind the breaches and what the motivations might have been. Theft of personally identifiable information (PII) may be used for identity theft and financially motivated cybercrime, such as credit card fraud. Many have speculated that the OPM data were taken for espionage rather than for criminal purposes, however, and some have cited China as the source of the breaches.

It remains unclear how the data from the OPM breaches might be used if they are indeed now in the hands of the Chinese government. Some suspect that the Chinese government may build a database of U.S. government employees that could help identify U.S. officials and their roles or that could help target individuals to gain access to additional systems or information. National security concerns include whether hackers could have obtained information that could help them identify clandestine and covert officers and operations.

The cybersecurity of most federal information systems is governed by the Federal Information Security Management Act (FISMA, 44 U.S.C. §3551 et seq.). Questions for policymakers include whether existing provisions of law give agencies the legislative authority and resources they need to adequately address the risks of future intrusions. In addition, effective sharing of cybersecurity information has been considered an important tool for protecting information systems from unauthorized intrusions and exfiltration of data. The 114th Congress is considering legislation to reduce perceived barriers to information sharing among private-sector entities and between them and federal agencies.

Contents

Contacts

On June 4, 2015, the U.S. Office of Personnel Management (OPM) revealed that a cyber intrusion into its information technology systems and data "may have compromised the personal information of [approximately 4.2 million] current and former Federal employees."[1] Later in June, OPM reported a separate cyber incident, which it said had compromised its databases housing background investigation records and resulted in the theft of sensitive information of 21.5 million individuals.[2]

The OPM breach, one of the largest reported on federal government systems, was detected partly through the use of the Department of Homeland Security's (DHS's) Einstein system—an intrusion detection system that "screens federal Internet traffic to identify potential cyber threats."[3] Reportedly, the hackers used compromised security credentials—those assigned to a KeyPoint Government Solutions employee, a federal background check contractor working on OPM systems—to exploit OPM's systems and gain access.[4] Officials do not believe that the intruders are still in the system.[5]

In the aftermath of the intrusions, Katherine Archuleta has stepped down as the director of OPM amid criticisms of how the agency managed its response to the intrusions and secured its information systems. Beth Cobert has taken on the role of acting director. In addition, OPM's Electronic Questionnaires for Investigations Processing (e-QIP) application, the "web-based automated system that was designed to facilitate the processing of standard investigative forms used when conducting background investigations," has been taken offline for "security enhancements."[6]

Notably, as is common with data breaches, available information on the recent OPM breach developments remains incomplete. Assumptions about the nature, origins, extent, and implications of the data breach may change, and some media reporting may conflict with official statements. Policymakers have received official briefings on the breach developments, and Congress has held a number of hearings on the issue.[7] This report provides an overview of the current understanding of the recent OPM breaches, as well as issues and questions raised about the source of the breaches, possible uses of the information exfiltrated, potential national security ramifications, and implications for the cybersecurity of federal information systems.

---

[1] Office of Personnel Management, "OPM to Notify Employees of Cybersecurity Incident," press release, June 4, 2015.

[2] Office of Personnel Management, "OPM Announces Steps to Protect Federal Workers and Others From Cyber Threats," press release, July 9, 2015.

[3] Ken Dilanian and Ricardo Alonso-Zaldivar, "Federal Data Compromised at OPM and Interior," *Associated Press*, June 4, 2015.

[4] See, for example, testimony at U.S. Congress, House Committee on Oversight and Government Reform, *OPM: Data Breach*, 114th Cong., 1st sess., June 16, 2015.

[5] Office of Personnel Management, *Information About OPM Cybersecurity Incidents*, https://www.opm.gov/cybersecurity/.

[6] Office of Personnel Management, *e-QIP Application*, https://www.opm.gov/investigations/e-qip-application/.

[7] See for example, U.S. Congress, House Committee on Oversight and Government Reform, *OPM: Data Breach*, 114th Cong., 1st sess., June 16, 2015; U.S. Congress, House Committee on Oversight and Government Reform, *OPM Data Breach: Part II*, 114th Cong., 1st sess., June 24, 2015; U.S. Congress, House Committee on Science, Space, and Technology, Subcommittee on Research and Technology and Subcommittee on Oversight, *Is the OPM Data Breach the Tip of the Iceberg?*, 114th Cong., 1st sess., July 8, 2015; U.S. Congress, Senate Committee on Homeland Security and Governmental Affairs, *Under Attack: Federal Cybersecurity and the OPM Data Breach*, 114th Cong., 1st sess., June 25, 2015; and U.S. Congress, Senate Committee on Appropriations, Subcommittee on Financial Services and General Government, *OPM Information Technology Spending and Data Security*, 114th Cong., 1st sess., June 23, 2015.

Exposed and Compromised Data

Information released in June 2015 regarding the first OPM breach indicates that hackers gained access to personal information including "employees' Social Security numbers, job assignments, performance ratings and training information."[8] The second reported breach involved the theft of data on 19.7 million current, former, and prospective employees and contractors *who applied for a background investigation* in 2000 or after using certain OPM forms.[9] This second breach also impacted personal information of 1.8 million non-applicants; OPM notes that these non-applicants are primarily individuals married to or otherwise cohabitating with background investigation applicants. OPM confirmed that "the usernames and passwords that background investigation applicants used to fill out their background investigation forms were also stolen."[10] About 1.1 million stolen records also include fingerprints.[11]

Notably, the two breaches revealed in June 2015 are not the first incidents targeting OPM databases containing such sensitive information. In a previous 2014 breach of OPM, hackers purportedly targeted "files on tens of thousands of employees who [had] applied for top-secret security clearances."[12]

Attribution and Links to China?

Determining an actor (and actor's motivation) involved in a cyber incident can help guide how the United States responds. If a perpetrator is believed to be motivated by profit or economic advantage, the investigation and response may be led by law enforcement using the tools of the criminal justice system. If the perpetrator is deemed to be a state-sponsored actor with a different motivation, the United States may utilize diplomatic or military tools in its response.

Speaking at an intelligence conference on June 24, 2015, Admiral Michael Rogers, director of the National Security Agency and head of U.S. Cyber Command, declined to discuss who might be responsible for the attacks, stating "I'm not [going to] get into the specifics of attribution.... That's a process that we're working through on the policy side. There's a wide range of people, groups and nation states out there aggressively attempting to gain access to that data."[13] Speaking at the same conference a day later, however, Director of National Intelligence James Clapper identified China as the "leading suspect" in the attacks. Mr. Clapper expressed grudging admiration for the alleged hackers, noting "[y]ou have to kind of salute the Chinese for what they did.... You know, if we had an opportunity to do that, I don't think we'd hesitate for a moment."[14]

---

[8] Ellen Nakashima, "Chinese Breach Data of 4 Million Federal Workers," *The Washington Post*, June 4, 2015.

[9] These include the SF-85, SF-85P, and SF-86 forms. They apply to applications for non-sensitive positions, public trust positions, and national security positions.

[10] Office of Personnel Management, "OPM Announces Steps to Protect Federal Workers and Others From Cyber Threats," press release, July 9, 2015.

[11] Ibid.

[12] Michael S. Schmidt, David E. Sanger, and Nicole Perlroth, "Chinese Hackers Pursue Key Data on U.S. Workers," *The New York Times*, July 9, 2014.

[13] David Welna, "In Data Breach, Reluctance to Point the Finger at China," National Public Radio, July 2, 2015.

[14] Ibid.

Without explicitly denying involvement, China has called speculation about its role in the OPM breaches neither "responsible nor scientific."[15] In late June 2015, top officials from the United States and China met in Washington, DC, for the annual session of the U.S.-China Strategic & Economic Dialogue—the two countries' most high-level dialogue. The dialogue included discussion of cyber issues, but progress on these issues was not mentioned among the dialogue's official "outcomes."[16] China said in early July that it was "imperative to stop groundless accusations, step up consultations to formulate an international code of conduct in cyberspace and jointly safeguard peace, security, openness and cooperation of the cyber space through enhanced dialogue and cooperation in the spirit of mutual respect."[17]

Of note, the United States in May 2014 filed criminal charges over a set of computer intrusions allegedly from China. The U.S. Department of Justice indicted five members of China's People's Liberation Army (PLA) for commercial cyber espionage that allegedly targeted five U.S. firms and a labor union.[18] It was the first, and so far only, time the United States has filed criminal charges against known state actors for cyber economic espionage.[19]

Criminal charges appear to be unlikely in the case of the OPM breach. As a matter of policy, the United States has sought to distinguish between cyber intrusions to collect data for national security purposes—to which the United States deems counterintelligence to be an appropriate response—and cyber intrusions to steal data for commercial purposes—to which the United States deems a criminal justice response to be appropriate. Describing discussions with Chinese officials at the July 2013 session of the annual U.S.-China Strategic & Economic Dialogue, a month after Edward Snowden made public documents related to U.S. signals intelligence, a senior Obama Administration stated, "[W]e were exceptionally clear, as the President has been, that there is a vast distinction between intelligence-gathering activities that all countries do and the theft of intellectual property for the benefit of businesses in the country, which we don't do and we don't think any country should do."[20] The OPM breach so far appears to be seen in the category of intelligence-gathering, rather than commercial espionage.

---

[15] Ministry of Foreign Affairs of the People's Republic of China, "Foreign Ministry Spokesperson Hong Lei's Regular Press Conference," June 5, 2015.

[16] U.S. Department of State, "U.S.-China Strategic & Economic Dialogue Outcomes of the Strategic Track," June 24, 2015, and U.S. Department of the Treasury, "2015 U.S.-China Strategic and Economic Dialogue U.S. Fact Sheet—Economic Track," June 25, 2015.

[17] Ministry of Foreign Affairs of the People's Republic of China, "Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference," July 10, 2015.

[18] United States District Court Western District of Pennsylvania, United States of America v. Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunhui, May 1, 2014.

[19] Department of Justice, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," press release, May 19, 2014.

[20] U.S. Department of State, "Senior Administration Officials on the First Day of the Strategic and Economic Dialogue and U.S.-China Relations," press release, July 10, 2013, http://www.state.gov/r/pa/prs/ps/2013/07/211801.htm. See also White House Office of the Press Secretary, "Signals Intelligence Activities," Presidential Policy Directive/PPD-28, January 17, 2014, https://www.whitehouse.gov/sites/default/files/docs/2014sigint_mem_ppd_rel.pdf; it states that, "The collection of signals intelligence is necessary for the United States to advance its national security and foreign policy interests and to protect its citizens and the citizens of its allies and partners from harm." The PPD also states, however, that, "The collection of foreign private commercial information or trade secrets is authorized only to protect the national security of the United States or its partners and allies. It is not an authorized foreign intelligence or counterintelligence purpose to collect such information to afford a competitive advantage to U.S. companies and U.S. business sectors commercially."

If the United States chooses to respond in other ways to intrusions from China, experts have suggested that China has multiple vulnerabilities that the United States could exploit. "China's uneven industrial development, fragmented cyber defenses, uneven cyber operator tradecraft, and the market dominance of Western information technology firms provide an environment conducive to Western CNE [computer network exploitation] against China," notes one scholar of Chinese cyber issues.[21]

Uses of Stolen OPM Data

It remains unclear how data from the OPM breaches might be used if they are indeed now in Chinese government hands. Experts in and out of government suspect that "China may be trying to build a giant database of federal employees" that could help identify U.S. officials and their roles.[22] Writing in *Wired* magazine, Senator Ben Sasse observed, "China may now have the largest spy-recruiting database in history."[23] There have been suggestions that information exposed in the breaches "could be useful in crafting 'spear-phishing' e-mails, which are designed to fool recipients into opening a link or an attachment so that the hacker can gain access to computer systems."[24]

In addition to being used by nation states, a trove of data from breaches such as those at OPM can provide a number of avenues for criminals to exploit. For instance, compromised Social Security numbers and other personally identifiable information (PII) may be used for identity theft[25] and financially motivated cybercrime, such as credit card fraud.[26] However, experts have been skeptical as to whether compromised information from the OPM breaches will even appear for sale in the online black market. When cybercriminals have tried in the underground markets to pass off other stolen data as that coming from the OPM breaches, this has been debunked, and the stolen data were shown to have come from other sources.[27] The lack of stolen OPM data appearing in the criminal underworld has led some to speculate the breaches were more likely conducted for espionage rather than criminal purposes. Nonetheless, even if data were stolen for non-criminal purposes, they could still fall into criminal hands.

While discussion about the stolen fingerprint information has been limited, analysts have begun to question how this data could be used. Some have speculated that if the fingerprints are of high enough quality, there may be "acutely negative long-term consequences for individuals affected and their future use of fingerprints to verify their identities."[28] Depending on whose hands the

[21] Jon R. Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction," International Security, Vol. 39, No. 3 (Winter 2014/2015), pp. 7-47, http://www.mitpressjournals.org/doi/abs/10.1162/ISEC_a_00189#.VaU3fflVhBc.

[22] Kevin Liptak, Theodore Schleifer, and Jim Sciutto, "China May Be Building Vast Database of Federal Worker Info, Experts Say," CNN.com, June 6, 2015, http://www.cnn.com/2015/06/04/politics/federal-agency-hacked-personnel-management/index.html.

[23] Senator Ben Sasse, "Senator Sasse: The OPM Hack May Have Given China a Spy Recruiting Database," *Wired*, July 9, 2015.

[24] Ellen Nakashima, "Chinese Breach Data of 4 Million Federal Workers," *The Washington Post*, June 4, 2015.

[25] For more information on identity theft, see CRS Report R40599, *Identity Theft: Trends and Issues*, by Kristin Finklea.

[26] For more information on cybercrime, see CRS Report R42547, *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement*, by Kristin Finklea and Catherine A. Theohary.

[27] Brian Krebs, "OPM's Database for Sale? Nope, It Came from Another US .Gov," *Krebs On Security*, June 18, 2015.

[28] Andrea Peterson, "The OPM Breach Exposed More Than a Million Fingerprints. Here's Why That['s] Terrible News," *The Washington Post*, July 15, 2015.

fingerprints come into, they could be used for criminal or counterintelligence purposes. For instance, they could be trafficked on the black market for profit or used to reveal the true identities of undercover officials. Also a concern is that biometric data such as fingerprints cannot be reissued—unlike other identifying information such as Social Security numbers.[29] This could make recovery from the breach more challenging for some.

National Security Implications

Reports have emerged indicating that OPM had attempted to take over the administration of Scattered Castles—the intelligence community's (IC's) database of sensitive clearance holders—and create a single clearance system for government employees. Although the IC refused out of concerns of increased vulnerability to hacking, news reports allege that some sharing of information between systems was underway by 2014. U.S. officials have denied that Scattered Castles was affected by the OPM hack, but they have neither confirmed nor denied that the databases were linked.[30]

If the IC's database were linked with OPM's, this could potentially help the hackers gain access to intelligence agency personnel and identify clandestine and covert officers. Even if data on intelligence agency personnel were not compromised, the hackers might be able to use the sensitive personnel information to "neutralize" U.S. officials by exploiting their personal weaknesses and/or targeting their relatives abroad.[31] Access to the IC's database could also reveal the process and criteria for gaining clearances and special access, allowing foreign agents to more easily infiltrate the U.S. government.

Some in the national security community have compared the potential damage of the OPM breaches to U.S. interests to that caused by Edward Snowden's leaks of classified information from the National Security Agency.[32] Yet the potential exists for damage beyond mere theft of classified information, including data manipulation or misinformation. While there is no evidence to suggest that this has happened, hackers would have had the ability, some say, while in U.S. systems to alter personnel files and create fictitious ones that would have gone undetected as far back as 2012.[33] Another concern is the possibility for data publication, as was done with the Snowden records. Dissemination of sensitive personnel files could damage the ability of

[29] Dustin Volz, "How Much Damage Can the OPM Hackers Do With a Million Fingerprints?," *National Journal*, July 14, 2015.

[30] See, for example, Natasha Bertrand, "US Officials investigating China's epic hack 'either need serious help or need to come clean now'," Business Insider, June 30, 2015. According to the Office of the Director of National Intelligence's (ODNI's) 2014 Report on Security Clearance Determinations, the two systems are not "linked," per se. In FY2014, OPM began sending information on active clearances from its Central Verification System to the Intelligence Community's Scattered Castles system. This is done, in part, so that ODNI can accurately assess the total number of active security clearances. It's not clear whether any information is shared in the other direction. See Office of the Director of National Intelligence, *2014 Report on Security Clearance Determinations*, April 2015.

[31] War On The Rocks, "The 9 Scariest Things That China Could Do With The OPM Security Clearance Data," July 2, 2015.

[32] Ryan Evans, "Why the Latest Government Hack is Worse Than the Snowden Affair," *The Washington Post*, June 17, 2015.

[33] Shane Harris, "Spies Warned Feds About OPM Mega-Hack Danger," *The Daily Beast*, June 30, 2015. See also Jani Antikainen and Pasi Eronen, "What's Worse Than Losing Your Data? Losing Your Trust in It," *Overt Action*, July 12, 2015.

clearance holders to operate with cover, and could open them up to potential exploitation from foreign intelligence agents.

Protecting Federal Information Systems

The cybersecurity of most federal information systems is governed by the Federal Information Security Management Act (FISMA, 44 U.S.C. §3551 et seq.),[34] which was updated at the end of the 113th Congress (P.L. 113-283).[35] The update gave explicit operational authority to DHS for implementation, including the authority to issue binding operational directives,[36] and it set requirements for breach notification for federal agencies. In addition, 40 U.S.C. §11319, as added by P.L. 113-291, provided agency chief information officers (CIOs) with additional budgeting and program authorities. A potential question for Congress is whether those and other provisions of law give agencies the legislative authority and resources they need to adequately address the risks of future intrusions. Among the specific questions Congress might consider are the following:

- Are the current authorities and requirements under FISMA sufficient, if fully implemented, to protect federal systems from future intrusions such as the most recent OPM intrusions? If not, what changes are needed to sufficiently reduce the level of risk? For example, should the priority level for cybersecurity be elevated with respect to other aspects of mission fulfillment; should the federal government adopt the explicit goal of being assessed by independent experts as having world-class cybersecurity?
- What are the barriers to improving federal cybersecurity to a level that would sufficiently reduce the risks of incidents such as the breaches at OPM, and what legislative actions are needed to remove them? For example, do agency heads, responsible for cybersecurity under FISMA, have sufficient understanding of cybersecurity to execute those responsibilities effectively—a broadly held concern with respect to private-sector chief executive officers that the National Institute of Standards and Technology (NIST) Cybersecurity Framework was designed in part to help address?[37] Are the recent amendments to CIO authorities sufficient for them to implement their cybersecurity responsibilities under FISMA?
- Does DHS have sufficient authorities to protect federal civilian systems under its statutory responsibilities? For example, should it have greater legislative authority to deploy countermeasures on federal systems, as some legislative proposals would provide?[38]

[34] FISMA largely does not apply to national security systems, which fall under the Committee on National Security Systems.

[35] For other relevant statutes, see CRS Report R42114, *Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation*, by Eric A. Fischer.

[36] The first directive, issued in May 2015, requires agencies to promptly correct vulnerabilities discovered in regular scans by DHS of public-facing agency websites.

[37] National Institute of Standards and Technology, "Cybersecurity Framework," August 26, 2014; see also CRS Report R42984, *The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress*, by Eric A. Fischer et al.

[38] See, for example, proposals in the 112th Congress, such as S. 3414, and an Obama Administration proposal (available at http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/law-enforcement-provisions-related-to-(continued...)

- Are the specific actions taken and proposed by the Obama Administration in the wake of the OPM breaches, such as the "cybersecurity sprint" and the proposed strategy and acquisition guidance initiatives,[39] sufficient to provide the required improvements in cybersecurity at federal agencies?

Congress is currently considering legislation to reduce perceived barriers to information sharing among private-sector entities and between them and federal agencies.[40] An additional potential question for Congress is whether the protections outlined in the proposed bills against inadvertent disclosure by federal agencies will be sufficient in the wake of breaches such as those involving OPM.

Author Contact Information

Kristin Finklea, Coordinator
Specialist in Domestic Security

Susan V. Lawrence
Specialist in Asian Affairs

Michelle D. Christensen
Analyst in Government Organization and Management

Catherine A. Theohary
Specialist in National Security Policy and Information Operations

Eric A. Fischer
Senior Specialist in Science and Technology

(...continued)

computer-security-full-bill.pdf).

[39] Tony Scott, "Fact Sheet: Enhancing and Strengthening the Federal Government's Cybersecurity," *OMBlog*, June 17, 2015; The White House, "Fact Sheet: Administration Cybersecurity Efforts 2015," press release, July 9, 2015.

[40] CRS Report R44069, *Cybersecurity and Information Sharing: Comparison of Legislative Proposals in the 114th Congress*, by Eric A. Fischer and Stephanie M. Logan.