0-The Washington Post-Hacks of OPM

Hacks of OPM databases compromised 22.1 million people, federal authorities say

By Ellen Nakashima

July 9, 2015

Two major breaches last year of U.S. government databases holding personnel records and security-clearance files exposed sensitive information about at least 22.1 million people, including not only federal employees and contractors but their families and friends, U.S. officials said Thursday.

The total vastly exceeds all previous estimates, and marks the most detailed accounting by the Office of Personnel Management of how many people were affected by cyber intrusions that U.S. officials have privately said were traced to the Chinese government.

[What you need to know about the hack of government background investigations]

But even beyond the rising number of apparent victims, U.S. officials said the breaches rank among the most potentially damaging cyber heists in U.S. government history because of the abundant detail in the files. Officials said hackers accessed not only personnel records of current and former employees but also extensive information about friends, relatives and others

listed as references in applications for security clearances for some of the most sensitive jobs in government.

[Chinese hack of personnel files includes security clearance database]

“It is a very big deal from a national security perspective and from a counterintelligence perspective,” FBI Director James B. Comey said at a meeting with reporters Thursday at the FBI headquarters. “It’s a treasure trove of information about everybody who has worked for, tried to work for, or works for the United States government.”

Other U.S. officials said that a foreign intelligence service could use the information to identify U.S. intelligence operatives, and that China is suspected of stealing large amounts of data on Americans as part of a “strategic plan” to increase its intelligence collection.

The OPM release came after a months-long effort by the agency to take inventory of the damage, an endeavor that required surveying enormous and often outdated computer systems.

The vast majority of those affected — 21.5 million people — were included in an OPM repository of security clearance files, officials said. At least 4.2 million people were affected by the breach of a separate database containing personnel records including Social Security numbers, job assignments and performance evaluations.

About 3.6 million of those affected were in both systems, an overlap that accounts for the 22.1 million total, officials said.

The hackers’ access was so extensive that U.S. officials said they think it is “highly likely” that every file associated with an OPM-managed security

clearance application since 2000 was exposed. Background checks before that time were less likely to be affected, officials said.

The CIA, largely appears to have been shielded from damage, especially for employees who have never worked at any other agency, officials said.

[Officials: Hackers had access to security data for a year]

Even so, some U.S. officials have said that a foreign spy service might be able to identify U.S. intelligence operatives by scrutinizing the OPM files. Names that appear on rosters of U.S. embassies but are missing from the OPM records might, through a process of elimination, reveal the identities of CIA operatives serving under diplomatic cover.

“That’s not conclusive that the person might be undercover CIA,” said one U.S. official, who spoke on the condition of anonymity to discuss the sensitive topic. “But it’s certainly worth taking a look at.”

Of those whose data was in the OPM background-check system, 19.7 million had applied for a security clearance. An additional 1.8 million were spouses, family members and other non-applicants, officials said.

Also exposed were 1.1 million sets of fingerprints, detailed financial and health records, and computer usernames and passwords that applicants used to fill out their security-clearance forms online.

OPM Director Katherine Archuleta indicated during a conference call with reporters that there is no evidence that the breach has been exploited for criminal purposes, saying, “There is no information at this time to suggest any misuse.”

[Watchdog: Shutdown of security clearance system “reactive” not “proactive”]

The U.S. government has said it will offer the affected employees at least three years of credit monitoring and other identity-protection services. *[Rebuild]* But OPM faces rising anger among members of federal employee unions who say they have received scant information about the breaches. *[Anger]*

Two class-action lawsuits have been filed against the agency and Archuleta *[Legal Action]*.

“Today’s new number is staggering,” said William R. Dougan *[Disappointment]*, president of the National Federation of Federal Employees. He added that “it is not yet clear how OPM can handle this massive increase, when they were already struggling with the initial 4.2 million. Now, not only do federal employees have to worry about their own personal information being exposed – but they must also worry about their spouse and children having their information compromised.” *[Worry]*

The White House is said to be weighing how to respond to what is being considered an aggressive act of espionage. U.S. officials said options include covert cyber-measures as well as punitive economic sanctions, although the nation’s ability to claim outrage has been undermined by the exposure of its own global spying programs by former intelligence contractor Edward Snowden.

Those responsible for the hack appear to have had access to OPM records for months. U.S. officials said the theft of security-clearance data took place over a six-month stretch that ended in January. The personnel records were stolen from October to April.

The breach of personnel records was discovered in April as a result of new cybersecurity tools OPM had installed, *[Reinforce]* said Andy Ozment, the Department of Homeland Security's assistant secretary for cybersecurity.

Officials said the thieves broke in by using stolen contractor logins and passwords. Although U.S. officials have said the intrusions were traced to the Chinese government, the Obama administration has not formally accused Beijing.

Comey said he thinks the hackers have obtained his "SF 86," referring to Standard Form 86, which all applicants for security clearances must fill out.

"If you have my SF 86, you know every place I've lived since I was 18, contact people at those addresses, neighbors at those addresses, all of my family, every place I've traveled outside the United States," Comey said. "Just imagine if you were a foreign intelligence service and you had that data." *[Worry]*

One of the major U.S. concerns is that an adversary could use the data to identify U.S. government employees who might be susceptible to pressure or inducements to engage in espionage. *[Worry]*

Thursday's disclosures prompted renewed calls among some on Capitol Hill for the resignation Archuleta and her chief information officer, Donna Seymour.

"Director Archuleta's slow and uneven response has not inspired confidence that she is the right person to manage OPM through this crisis," said Sen. Mark R. Warner *[Anger]* (D-Va.), a member of the Senate Intelligence Committee. "It is time for her to step down, and I strongly urge the administration to choose new management with proven abilities to

address a crisis of this magnitude with an appropriate sense of urgency and accountability."

Archuleta said that she will not step down, and that she remains "committed to the work that I am doing at OPM."

Advertisement

Agency officials say that it was only because of a strategic plan put in place by Archuleta shortly after she became director in November 2014 that the breaches were discovered.

"There are certainly some people I would like to see given the boot for not paying attention to cybersecurity, but Katherine Archuleta is not one of them," said one administration official, requesting anonymity to discuss personnel issues. "Maybe they didn't move as fast as they should have *[Disappointment]* but they were at least moving in the right direction and were prioritizing it in an agency that didn't think of itself as having a security mission." *[Positive]*

It has taken weeks for the agency to come up with the number, in large part because of the difficulty, officials say, of reviewing data contained in numerous computers that make up the background check system. Many of the computers are antiquated. There were many instances of names being duplicated — sometimes because someone was listed as a reference in several background checks as well as having their own clearance.

"The forensics for that …investigation were extremely complicated," Ozment said.

In weighing how to respond, some U.S. officials caution against taking actions against foreign states when the cyber theft is conducted for traditional spying motives. The United States has not officially named China or the motive, but privately officials say it appears China was conducting a form of traditional espionage.

"I think we have to be careful about the importance of continuing to draw a line between theft for economic advantage and traditional foreign

intelligence activities, which may look untraditional now that they're in the cyber realm," said Rep. Adam Schiff (D-Calif.), a member of the House Intelligence Committee. "We want to draw a bright line" that hacking for economic benefit "is a violation of international norms."

If the United States blurs the line between economic spying and foreign intelligence spying, "we risk undermining the fight against economic theft."

He said rather than "simply place blame on the hackers, we need to acknowledge our own culpability in failing to adequately protect so obvious a target. Plainly, we need to do so much more to safeguard our networks." *[Disappointment]*

The government has already begun taking steps to mitigate the damage in the intelligence and counterintelligence arena *[Rebuild]*, Schiff said. "We're going to be doing that for years, in terms of the whole range of steps that we'll have to take to protect our people and our sources and methods."

He added: "The consequences will be very far-reaching."

Lisa Rein contributed to this story.