China suspected in massive breach of federal personnel data (Update)

June 4 2015, byKen Dilanian And Ricardo Alonso-Zaldivar

This Feb. 24, 2015, file photo, shows the Homeland Security Department headquarters in northwest Washington. The Department of Homeland Security said in a statement Thursday, June 4, 2015, that data from the Office of Personnel Management and the Interior Department had been hacked. (AP Photo/Manuel Balce Ceneta, File)

China-based hackers are suspected of breaking into the computer networks of the U.S. government personnel office and stealing

identifying information of at least 4 million federal workers, American officials said Thursday.

The Department of Homeland Security said in a statement that data from the Office of Personnel Management and the Interior Department had been compromised.

"The FBI is conducting an investigation to identify how and why this occurred," the statement said.

The hackers were believed to be based in China, said Sen. Susan Collins, a Maine Republican.

Collins, a member of the Senate intelligence committee, said the breach was "yet another indication of a foreign power probing successfully and focusing on what appears to be data that would identify people with security clearances."

A spokesman for the Chinese Embassy in Washington called such accusations "not responsible and counterproductive."

"Cyberattacks conducted across countries are hard to track and therefore the source of attacks is difficult to identify," spokesman Zhu Haiquan said Thursday night. He added that hacking can "only be addressed by international cooperation based on mutual trust and mutual respect."

A U.S. official, who declined to be named because he was not authorized to publicly discuss the data breach, said it could potentially affect every federal agency. One key question is whether intelligence agency employee information was stolen. Former government employees are affected as well.

"This is an attack against the nation," said Ken Ammon, chief strategy

officer of Xceedium, who said the attack fit the pattern of those carried out by nation states for the purpose of espionage. The information stolen could be used to impersonate or blackmail federal employees with access to sensitive information, he said.

The Office of Personnel Management is the human resources department for the federal government, and it conducts background checks for security clearances. The OPM conducts more than 90 percent of federal background investigations, according to its website.

The agency said it is offering credit monitoring and identity theft insurance for 18 months to individuals potentially affected. The National Treasury Employees Union, which represents workers in 31 federal agencies, said it is encouraging members to sign up for the monitoring as soon as possible.

In November, a former DHS contractor disclosed another cyberbreach that compromised the private files of more than 25,000 DHS workers and thousands of other federal employees.

Cyber-security experts also noted that the OPM was targeted a year ago in a cyber-attack that was suspected of originating in China. In that case, authorities reported no personal information was stolen.

One expert said it's possible that hackers could use information from government personnel files for financial gain. In a recent case disclosed by the IRS, hackers appear to have obtained tax return information by posing as taxpayers, using personal information gleaned from previous commercial breaches, said Rick Holland, an information security analyst at Forrester Research.

"Given what OPM does around security clearances, and the level of detail they acquire when doing these investigations, both on the subjects

of the investigations and their contacts and references, it would be a vast amount of information," Holland added.

DHS said its intrusion detection system, known as EINSTEIN, which screens federal Internet traffic to identify potential cyber threats, identified the hack of OPM's systems and the Interior Department's data center, which is shared by other federal agencies.

It was unclear why the EINSTEIN system didn't detect the breach until after so many records had been copied and removed.

"DHS is continuing to monitor federal networks for any suspicious activity and is working aggressively with the affected agencies to conduct investigative analysis to assess the extent of this alleged intrusion," the statement said.

Cybersecurity expert Morgan Wright of the Center for Digital Government, an advisory institute, said EINSTEIN "certainly appears to be a failure at this point. The government would be better off outsourcing their security to the private sector where's there at least some accountability."

Rep. Adam Schiff, ranking Democrat on the House intelligence committee, called the hack "shocking, because Americans may expect that federal computer networks are maintained with state of the art defenses."

Ammon said federal agencies are rushing to install two-factor authentication with smart cards, a system designed to make it harder for intruders to access networks. But implementing that technology takes time.

Senate Intelligence Committee Chairman Richard Burr, R-N.C., said the

government must overhaul its cybersecurity defenses. "Our response to these attacks can no longer simply be notifying people after their personal information has been stolen," he said. "We must start to prevent these breaches in the first place."

___

Associated Press writers Donna Cassata, Alicia A. Caldwell and Kevin Freking in Washington and Brandon Bailey in San Francisco contributed to this report.

___

Follow Ken Dilanian on Twitter at twitter.com/KenDilanianAP