Cybertheft of personnel info rips hole in espionage defenses

June 16 2015, byKen Dilanian

In this April 22, 2015 file photo, House Oversight Committee Chairman Rep. Jason Chaffetz, R-Utah, speaks on Capitol Hill in Washington. When hackers broke into a database filled with the private information of U.S. security clearance holders, they likely got access to the names of foreign relatives of some of those officials who are living abroad. "It may be the single biggest breach of data that our government has ever had," said Chaffetz on teh C-SPAN Newsmakers program, calling the stolen data "the most sensitive information we have." (AP Photo/Cliff Owen, File)

By exposing the names and addresses of foreign relatives, the cybertheft of private information on U.S. security clearance holders by hackers linked to China will complicate the deployment and promotion of American intelligence professionals with special language skills and diverse backgrounds, current and former U.S. officials say.

Officials fear that China will seek to gain leverage over Americans with access to secrets by pressuring their overseas relatives, particularly if they happen to be living in China or another authoritarian country. Over the last decade, U.S. intelligence agencies have sought to hire more people of Asian and Middle Eastern descent, some of whom have relatives living overseas. The compromise of their personal data is likely to place additional burdens on employees who already face onerous security scrutiny.

China denies involvement in the cyberattack that is being called the most damaging national security loss in more than a decade.

The potential for new avenues of espionage against the U.S. is among the most obvious repercussions of the pair of data breaches by hackers who are believed to have stolen personnel data on millions of current and former federal employees and contractors.

Officials from the Department of Homeland Security, which is in charge of defending civilian government networks from cyberattacks, and the Office of Personnel Management, which failed to protect its sensitive personnel information from hackers, are slated to discuss the loss Tuesday in front of the House Oversight and Government Reform Committee.

"It may be the single biggest breach of data that our government has ever had," Jason Chaffetz, a Utah Republican who chairs the oversight committee, said on the C-SPAN Newsmakers program over the

weekend, calling the stolen data "the most sensitive information we have."

In the cyberattack targeting federal personnel records, hackers are believed to have obtained the Social Security numbers, birth dates, job actions and other private information on every federal employee and millions of former employees and contractors.

In a second attack, which the Obama administration acknowledged on Friday after downplaying the possibility for days, the cyberspies got detailed background information on millions of military, intelligence and other personnel who have been investigated for security clearances. Together, the hacks compromised the records of as many as 18 million people.

Applicants for security clearances are required to list drug use, criminal convictions, mental health issues, and the names and addresses of their foreign relatives.

"You're supposed to list every relative outside the U.S. who could be a source of foreign government pressure on you," said Stewart Baker, who served in senior roles at DHS and the National Security Agency.

The pitch to a Chinese-American working with U.S. secrets, he said, would amount to, "You belong to us, and we can make an approach that is designed to make you understand that."

But the fears don't end with China. China's intelligence service could share the information with allies such as North Korea or Pakistan. Also, experts say, many who hack on behalf of the Chinese government are allowed to freelance and sell what they steal.

"The 'friends and family' dataset is ultimately the most useful for a

hostile intelligence service," said Richard Zahner, a retired lieutenant general and former top NSA official. Tie the information to what's publicly available, and other intelligence the adversary has already collected, "and you have insights that few services have ever achieved."

Those insights go beyond merely spying on the U.S. government, he said. Many senior business executives need government clearances to serve on advisory boards, or hold them from prior government service. Google chairman Eric Schmidt, for example, holds a security clearance, he has said. So at one point did Microsoft founders Bill Gates and Steve Ballmer.

"If I can get into the strategic planning side of a U.S. competitor, investment decisions and negotiating strategies are vastly simplified," Zahner said.

Also Monday, DHS disclosed that as many as 390,000 employees, contractors and job applicants may have had their personal data breached in a separate hack of a contractor, KeyPoint Government Solutions, that was discovered in September. In December, DHS acknowledged another hack of the same contractor in which 48,000 people were affected.

Administration officials have left many questions unanswered, including why the latest hacks went undetected for months. The federal chief information officer, Tony Scott, ordered government agencies to beef up their network security by scanning logs, patching security holes, and accelerating their use authentication that goes beyond passwords.

But critics have likened those steps to closing the proverbial barn door after all the horses have bolted. They question why the government is not doing more to encrypt, or render in code, sensitive data.

"Man, I can't believe that stuff wasn't encrypted," Brian Kelly, chief security officer at Rackspace Inc. of San Antonio.

Organizations are too focused on firewalls, spam filters, and other Maginot Line-type defenses that have lost their effectiveness, Kelly said.

"That's a misguided philosophy," he said. "There's no such thing as a perimeter anymore."