Fed agency blames giant hack on 'neglected' security system

June 16 2015, byKen Dilanian

Office of Personnel Management (OPM) Director Katherine Archuleta testifies on Capitol Hill in Washington, Tuesday, June 16, 2015, before the before the House Oversight and Government Reform Committee hearing on the OPM data breach. 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. (AP Photo/Cliff Owen)

The agency that allowed hackers linked to China to steal private

information about nearly every federal employee—and detailed personal histories of millions with security clearances—failed for years to take basic steps to secure its computer networks, officials acknowledged to Congress on Tuesday.

Democrats and Republicans on the House Oversight and Government Reform Committee spoke in unison to describe their outrage over what they called gross negligence by the Office of Personnel Management. The agency's data was breached last year in two massive cyberattacks only recently revealed.

The criticism came from within, as well. Michael Esser, the agency's assistant inspector general for audit, detailed a yearslong failure by OPM to adhere to reasonable cybersecurity practices, and he said that that for a long time, the people running the agency's information technology had no expertise.

Last year, he said, an inspector general's audit recommended that the agency shut down some of its networks because they were so vulnerable. The director, Katherine Archuleta, declined, saying it would interfere with the agency's mission.

The hackers were already inside her networks, she later acknowledged.

"You failed utterly and totally," said committee Chairman Jason Chaffetz, a Utah Republican. "They recommended it was so bad that you shut it down and you didn't."

Archuleta, stumbling occasionally under withering questions from lawmakers, sought to defend her tenure and portray the agency's problems as decades in the making as its equipment aged. She appeared to cast blame on her recent predecessors, one of whom, John Berry, is the U.S. ambassador to Australia.

Offered chances to apologize and resign, she declined to do either.

Chaffetz said the two breaches "may be the most devastating cyberattack in our nation's history," and said OPM's security policy was akin to leaving its doors and windows unlocked and expecting nothing to be stolen.

"I am as distressed as you are about how long these systems have gone neglected," Archuleta said, adding at another point, "The whole of government is responsible and it will take all of us to solve the issue."

Archuleta and the other witnesses offered few new details about the breaches in the public hearing, deferring most questions about methods and damage to a later, classified session.

Michael Esser, assistant inspector general for Audits, Office of Inspector General, Office of Personnel Management. (OPM), testifies on Capitol Hill in

Washington, Tuesday, June 16, 2015, before the before the House Oversight and Government Reform Committee hearing on the OPM data breach. 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. (AP Photo/Cliff Owen)

After that session, Rep. Elijah Cummings of Maryland, the committee's ranking Democrat, demanded that the committee hear testimony from two OPM contractors, KeyPoint and USIS, that fell victim to hacks last year. Earlier, Cummings and other lawmakers questioned whether the OPM network was compromised first through hacking of the contractors, and OPM officials declined to answer.

During the open hearing, Donna Seymour, the agency's chief information officer, confirmed that personnel information on 4.2 million current and former federal employees had been stolen, not just accessed.

The number of security clearance holders whose data has been taken is not yet known, she said. But the records go back to 1985 and include contractors as well as federal employees. Some government officials estimate the number could be up to 14 million.

And because their security clearance applications contain personal information about friends and family, those people's data is vulnerable as well.

Seymour also disclosed that any federal employees who submitted service history records to OPM, whether or not their personnel records are kept by the agency, likely had their information stolen. That raised the specter that intelligence agency employees who were not kept in the

main personnel system for security reasons may have been exposed anyway.

Another fear is that covert intelligence officers working undercover as government employees may have been made vulnerable. If their names are not in the federal employee database, that could be revealing to foreign adversaries; there also could be holes in any bogus employee record built for spying cover purposes.

Andy Ozment, a top Department of Homeland Security cyber official, said the hackers gained access to OPM's network using stolen credentials.

That was important because many lawmakers and outside experts had criticized OPM for failing to take the obvious step of encrypting sensitive data, including Social Security numbers. Ozment said attackers with network credentials could have accessed encrypted data, anyway.

Rep. Will Hurd, a Texas Republican and former covert CIA officer, said he didn't doubt the good intentions of the OPM witnesses, but "the execution has been horrific."

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)

China denies involvement in the cyberattack, and no evidence has been aired publicly proving Chinese involvement although the government says it has "moderate confidence" China was involved.

Lawmakers voiced fears Tuesday that China will seek to gain leverage over Americans with access to secrets by pressuring their overseas relatives and contacts, particularly if they happen to be living in China or another authoritarian country.

"China now has a list of Chinese citizens worldwide who are in close contact with American officials and they can use that for espionage purposes," said Rep. Ron DeSantis, a Florida Republican.

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 the other attack, which the Obama administration acknowledged on Friday after downplaying the possibility for days, the cyber spies got detailed background information on millions of military, intelligence and other personnel who have been investigated for security clearances.

A chart of data breaches is shown on Capitol Hill in Washington, Tuesday, June 16, 2015, as witnesses testify before the House Oversight and Government Reform committee's hearing on the Office of Personnel Management (OPM)

data breach. (AP Photo/Cliff Owen)

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

"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."

The personnel records hack comes in a long line of other cyber breaches linked to China and targeting the personal information of Americans, including one in January against health insurer Anthem.

"The United States of America is under attack," Cummings said. "Sophisticated cyber spies, many from foreign countries, are targeting the sensitive personnel information of millions of Americans. They are attacking our government, our economy, our financial sector, our health care systems and virtually every single aspect of our lives."