Nobody at OPM to blame for massive data breach, director says

Erin Kelly, USA TODAY *2:53 p.m. EDT June 23, 2015*

(Photo: Cliff Owen, AP)

WASHINGTON — The director of the Office of Personnel Management said Tuesday she doesn't believe anyone at her agency is personally responsible for allowing the massive hack attack that has exposed the personal information of millions of federal employees.

"If there is anyone to blame, it is the perpetrators," OPM Director Katherine Archuleta told members of a Senate panel at the first of four congressional hearings this week to examine the OPM cyber attack..

House Oversight Committee Chairman Jason Chaffetz, R-Utah, and other lawmakers have called on Archuleta to resign in the wake of what has been described as the most devastating cyber attack in U.S. history.

USA TODAY

OPM still trying to determine how many hurt by hack

(http://www.usatoday.com/story/news/politics/2015/06/16/opm-hack-house-hearing-archuleta/71261820/)

"I don't believe anyone (at OPM) is personally responsible," Archuleta said in response to a question from Sen. Jerry Moran, R-Kan. "We're working as hard as we can to protect the data of our employees."

Archuleta also blamed "decades of lack of investment in IT systems." She is seeking a $32 million increase in OPM's 2016 budget, with most of the raise slated to pay for modernizing the agency's information technology.

However, Michael Esser, the OPM's assistant inspector general for audits, said that some of the systems that were breached were modern systems rather than the aging, decades-old mechanisms that Archuleta is trying to replace. He said most of the agency's cybersecurity problems are due to poor management.

"Although OPM has made progress in certain areas, some of the current problems and weaknesses were identified as far back as Fiscal Year 2007," Esser testified. "We believe this long history of systemic failures to properly manage its IT infrastructure may have ultimately led to the breaches we are discussing today."

Federal investigators are still trying to figure out how many federal employees are victims of two major hack attacks that compromised the OPM's records in late 2014 and early 2015.

Sen. John Boozman, R-Ark., speaks during a Senate Appropriations subcommittee hearing on June 23, 2015. *(Photo: Drew Angerer, Getty Images)*

Archuleta said that more than 4 million employees were affected by the first hack, which was discovered in April and publicly disclosed this month. OPM has net yet determined how many more were victimized in a second attack discovered in May, she said. Some news reports have suggested that the total number may be as high as 18 million people. OPM officials said some of the compromised employee data may go back as far as 30 years.

"What has happened at OPM is devastating," said Sen. John Boozman, R-Ark., chairman of the Appropriations Subcommittee on Financial Services and General Government, which held the hearing. "Millions of Americans and their families and friends have been affected."

He said that OPM's action to give federal employees free credit monitoring and identity theft insurance will not be enough "to address the long-term consequences that we may see for years to come."

Federal employees have questioned why OPM didn't encrypt their Social Security numbers to protect them from hackers. Archuleta said Tuesday that she's been told by government cyber experts that encryption wouldn't have been enough to protect the data that was compromised.

Esser said OPM needs to quickly employ an agency-wide system requiring employees to use at least two forms of identification — such as a security code and a card — to access sensitive government data.

Archuleta said the hackers breached the OPM data using security credentials from KeyPoint Government Solutions, which OPM hired to conduct background checks of current, former and prospective federal employees whose jobs require a security clearance.

USA TODAY

OPM hack raises questions about security of government contractors

(http://www.usatoday.com/story/news/politics/2015/06/20/opm-hack-government-contractors/28922679/)

Sen. Christopher Coons, D-Del., said Congress must pay for more IT investment at OPM, which began a three-year, $67 million IT modernization program in 2014 and is seeking a final installment of $21 million in 2016 to complete the project.

"We have to understand that without that funding, the investments of the past two years cannot be meaningfully completed," Coons said.

Archuleta said she may be coming back to Congress by the end of this week with a request for additional funds to deal with the aftermath of the data breach. She said it will cost about $20 million for OPM to notify federal employees that their records may have been compromised and to pay for credit reports and identity theft monitoring.

Republicans were skeptical that more investment in information technology is the the answer to OPM's cybersecurity problems.

"It's easy to suggest more money is the solution," Boozman said. "That seems to be the response the administration leans on every time there is a problem. But it is often the wrong choice, especially in situations like this where it appears that the problem is much greater than a lack of resources."

Boozman said the OPM hack underscores a larger, government-wide weakness with cybersecurity despite the fact that the government spends about $82 billion a year on information technology.

Nineteen of 24 major federal agencies have reported deficiencies in information security controls, Boozman said.

"How many headlines of serious data breaches will it take to implement the steps necessary to protect ourselves?" he asked.

Follow @ErinVKelly (https://twitter.com/erinvkelly) on Twitter

Read or Share this story: http://usat.ly/1N6y8Rw