

Agency chief: Contractor's credential used to breach system

June 23 2015, by Deb Riechmann And Ken Dilanian



Katherine Archuleta, director, Office of Personnel Management, testifies before the Senate Appropriations subcommittee on Financial Services and General Government hearing to review IT spending and data security at the OPM in Washington, Tuesday, June 23, 2015. (AP Photo/Cliff Owen)

The head of the government agency that suffered two massive cyberattacks said Tuesday that a hacker gained access to its records with a credential used by a federal contractor.

Despite calls for her ouster, the director of the Office of Personnel Management said if anyone is responsible for the breaches, it's the hackers.

Katherine Archuleta told a Senate hearing that old computer networks were to blame for the cyberbreak-ins that exposed private information on nearly every federal employee and personal histories of millions with security clearances.

"If there is anyone to blame, it's the perpetrators," she said.

Sen. John Boozman, R-Ark., the chairman of the Senate Appropriations Committee panel where she testified, said OPM officials are blaming antiquated systems, but not all the breaches occurred exclusively on older networks.

"I still don't think we know exactly what's gone on," Boozman said later in the afternoon on his way out of a classified briefing on cybersecurity.

Archuleta told a House oversight committee last week that many of the agency's systems were too old to support encryption, which would have made the data harder to steal. But the agency's independent watchdog is challenging that assessment in written testimony to be delivered Wednesday to the same committee.

OPM Inspector General Patrick McFarland says some of the systems involved in the data breach were modern, so encryption could have been used.

Boozman and other senators said there was concern that people who stole the information could use it to file fake tax returns with the Internal Revenue Service.

Sen. Susan Collins, R-Maine, said, "People would discover it because they would file their returns and the IRS would say, 'Oh, you've already filed, and we've already sent your return.' So this is really serious."

President Barack Obama has said he continues to have confidence in Archuleta, although several Republican and Democratic lawmakers have called on her to step down—the latest being Sen. Steve Daines, R-Mont.

"Under Katherine Archuleta's watch, OPM allowed one of the largest breaches of federal employees' personal information in our nation's history," Daines said Tuesday. "Ms. Archuleta has refused to take accountability for this great failure—in turn failing the American people, whom she swore an oath to protect and defend."

Daines, who worked in Montana's technology sector for more than 12 years, is among the Americans who received a notice that his information might have been compromised in the latest breach.

Archuleta testified that an "adversary" somehow obtained a user credential used by KeyPoint Government Solutions, a contractor based in Loveland, Colorado. She didn't say specifically when that occurred or if it was linked to the two cyberbreaches that exposed private information on nearly every federal employee and personal histories of millions with security clearances.

"I want to be very clear that while the adversary leveraged—compromised—a KeyPoint User credential to gain access to OPM's network, we don't have any evidence that would suggest that KeyPoint as a company was responsible or directly involved in the intrusion," she said.

The agency has not identified any "pattern or material deficiency" that led to the compromise, Archuleta said, and the company has actively

worked to secure its network and meet additional protective controls the government has asked.

Archuleta said the cyberattacks were discovered because of OPM's stepped-up efforts in the past 18 months to improve security, but she acknowledged the office still has work to do. She said that in fiscal 2014 and 2015, the agency committed nearly \$67 million toward shoring up its information technology infrastructure and in June of last year began completely redesigning the network.

She said that work is on schedule and on budget, that OPM has added firewalls and a better authentication process for remote access and that it is increasing the types of ways used to encrypt data. A new data center network is expected to be completed by the end of this fiscal year. The agency's budget request for fiscal 2016 includes an additional \$21 million above 2015 spending to further support modernization.

© 2015 The Associated Press. All rights reserved.

Citation: Agency chief: Contractor's credential used to breach system (2015, June 23) retrieved 25 April 2024 from <https://phys.org/news/2015-06-opm-chief-contractor-credential-breach.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.