US: More than 21 million affected by government data breach (Update)

July 9 2015, byJack Gillum And Josh Lederman

In this June 5, 2015, file photo, the Homeland Security Department headquarters in northwest Washington. The Obama administration says hackers stole Social Security numbers from more than 21 million people and took other sensitive information when government computer systems were compromised. The number affected by the breach is higher than the 14 million figure that investigators gave The Associated Press in June. (AP Photo/Susan Walsh, File)

Hackers stole Social Security numbers, health histories and other highly

sensitive data from more than 21 million people, the Obama administration said Thursday, acknowledging that the breach of U.S. government computer systems was far more severe than previously disclosed.

The scope of the data breach—believed to be the biggest in U.S. history—has grown dramatically since the government first disclosed earlier this year that hackers had gotten into the Office of Personnel Management's personnel database and stolen records for about 4.2 million people. Since then, the Obama administration has acknowledged a second, related breach of the systems housing private data that individuals submit during background investigations to obtain security clearances.

That second attack affected more than 19 million people who applied for clearances, as well as nearly 2 million of their spouses, housemates and others who never applied for security clearances, the administration said. Among the data the hackers stole: criminal, financial, health, employment and residency histories, as well as information about their families and acquaintances.

The new revelations drew indignation from members of Congress who have said the administration has not done enough to protect personal data in their systems, as well as calls for OPM Director Katherine Archuleta and her top deputies to resign. House Oversight and Government Reform Committee Chairman Jason Chaffetz, a Utah Republican, said Archuleta and her aides had "consciously ignored the warnings and failed to correct these weaknesses."

"Such incompetence is inexcusable," Chaffetz said in a statement.

House Republican leaders—Speaker John Boehner, Majority Leader Kevin McCarthy and Whip Steve Scalise—also called for Archuleta's

resignation and said President Barack Obama must "take a strong stand against incompetence."

Some Democrats weighed in against Archuleta as well. Virginia Sen. Mark Warner said, "It is time for her to step down, and I strongly urge the administration to choose new management with proven abilities to address a crisis of this magnitude with an appropriate sense of urgency and accountability."

Yet Archuleta insisted she would not step down. "I am committed to the work that I am doing," she said in a conference call with reporters.

Archuleta said the hackers also obtained user names and passwords that prospective employees used to fill out their background investigation forms, as well as the contents of interviews conducted as part of those investigations. Yet the government insisted there were no indications that the hackers have used the data they stole.

Still, the government declined to say who was behind the attack.

Numerous U.S. lawmakers, including Senate Democratic leader Harry Reid, have said China was behind the attack. But Michael Daniel, Obama's cybersecurity coordinator, said the government wasn't yet ready to say who was responsible.

"Just because we're not doing public attribution does not mean that we're not taking steps to deal with the matter," Daniel told reporters.

While officials would not point the finger at China, they acknowledged that the same party was responsible for both of the breaches, which took place in 2014 and early 2015. Investigators previously told The Associated Press that the U.S. government was increasingly confident that China's government, and not criminal hackers, was responsible for

the extraordinary theft of personal information.

China has publicly denied involvement in the break-in.

The administration said it has stepped up its cybersecurity efforts by proposing new legislation, urging private industry to share more information about attacks and examining how the government conducts sensitive background investigations.

"Each and every one of us at OPM is committed to protecting the safety and the security of the info that is placed in our trust," Archuleta said. In early June, government employees received notice that OPM would offer credit-monitoring services and identity-theft insurance to those affected.

Meanwhile, the White House waited about a month before telling the public that hackers had stolen the personal information of millions of people associated with the government, people directly involved with the investigation told the AP last month.

FBI Director James Comey, in a briefing with reporters Thursday, described the scope of the OPM breach as "huge" and called it "a very big deal from a national-security perspective and a counterintelligence perspective."

"It's a treasure trove of information about everybody who has worked for, tried to work for, or works for the United States government," he said.

© 2015 The Associated Press. All rights reserved.

Citation: US: More than 21 million affected by government data breach (Update) (2015, July 9) retrieved 26 April 2024 from https://phys.org/news/2015-07-huge-hack-affected-mn.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.