The New York Times | http://nyti.ms/1HiFLCZ

U.S.

Hacking of Government Computers Exposed 21.5 Million People

By JULIE HIRSCHFELD DAVIS JULY 9, 2015

WASHINGTON — The Obama administration on Thursday revealed that 21.5 million people were swept up in a colossal breach of government computer systems that was far more damaging than initially thought, resulting in the theft of a vast trove of personal information, including Social Security numbers and some fingerprints.

Every person given a government background check for the last 15 years was probably affected, the Office of Personnel Management said in announcing the results of a forensic investigation of the episode, whose existence was known but not its sweeping toll.

The agency said hackers stole "sensitive information," including addresses, health and financial history, and other private details, from 19.7 million people who had been subjected to a government background check, as well as 1.8 million others, including their spouses and friends. The theft was separate from, but related to, a breach revealed last month that compromised the personnel data of 4.2 million federal employees, officials said.

Both attacks are believed to have originated in China, although senior administration officials on Thursday declined to pinpoint a perpetrator, except to say that they had indications that the same actor carried out the two hacks.

The breaches constitute what is apparently the largest cyberattack into the systems of the United States government, providing a frightening glimpse of the technological vulnerabilities of federal agencies that handle sensitive information. They also seemed certain to intensify debate in Washington over what the government must do to address its substantial weaknesses in cybersecurity, long the subject of dire warnings but seldom acted upon by agencies, Congress or the White House.

"This incident that we are talking about today is unfortunately not without precedent," said Michael Daniel, the White House cybersecurity coordinator. "We have to raise our level of cybersecurity in both the private sector and the public sector."

In a conference call to detail the grim findings and announce the agency's response, Katherine Archuleta, the director of the Office of Personnel Management, said that she would not resign despite calls from members of Congress in both parties for her dismissal.

"I am committed to the work that I am doing at O.P.M.," she said. "We are working very hard, not only at O.P.M. but across government, to ensure the cybersecurity of all our systems, and I will continue to do so."

She announced new security measures that would be installed at the agency as well as free credit and identity theft monitoring for the victims of the breach, although she said there was "no information at this time to suggest any misuse or further dissemination of the information that was stolen from O.P.M.'s system."

Even so, national security officials have acknowledged the seriousness of the intrusion. Before the scope was made public on Thursday, James B. Comey, Jr., the director of the F.B.I., called the breach "a very big deal," noting that the information obtained included people's addresses; details on their neighbors, friends and relatives; their travel destinations outside the United States; and any foreigners they had come into contact with.

"There is a treasure trove of information about everybody who has worked for, tried to work for or works for the United States government," Mr. Comey said during a briefing. "Just imagine you are an intelligence service and you had that data, how it would be useful to you."

Administration officials said it was the personnel office's work to modernize its computer systems that first led it to detect the breach.

In April, the agency informed the Department of Homeland Security that it had found an intrusion, and the department went to work with the F.B.I. to learn more, said Andy Ozment, a top cybersecurity official at Homeland Security. That inquiry, he said, revealed that the intruder had broken into a network at the Interior Department that held a personnel office database, leading to the theft of records of 4.2 million current and former federal employees. It also found that there had been a computer intrusion at the personnel office itself, leading to the much larger trove of background check records.

Mr. Ozment said the hacker in both cases gained access to the computer systems "via a compromised credential of a contractor."

The debacle has touched off a scramble by federal officials to bolster the security of their networks. Tony Scott, the government's chief information officer, said every agency was racing to make improvements, including the use of basic tools like two-factor authentication that requires anyone with the password to a system to use a second, one-time password to log in from an unrecognized computer.

"This is important work across all of the agencies of the federal government to make sure that we greatly enhance the cybersecurity profile of the U.S. government as a whole," Mr. Scott said.

But that effort comes after almost two decades of warnings from government auditors and other internal investigations into the vulnerabilities

in federal agency networks. “There’s still much that agencies need to do that they are not doing to protect their systems,” said Gregory C. Wilshusen, the director of information security issues at the Government Accountability Office, which has conducted cyber audits for almost two decades.

Warnings from auditors about serious vulnerabilities are often ignored by agency officials, he added. “That’s been a recurring theme. They believe they’ve taken corrective actions, but when one goes back to check, we find that they haven’t.”

The revelations quickly prompted calls for the ouster of Ms. Archuleta, whose agency had been warned in a series of reports since 2007 about the many vulnerabilities on its antiquated computer systems.

Representative Jason Chaffetz, Republican of Utah and the chairman of the House Oversight and Government Reform Committee, said Ms. Archuleta and her top technology official should resign or be removed.

“Their negligence has now put the personal and sensitive information of 21.5 million Americans into the hands of our adversaries,” Mr. Chaffetz said. “Such incompetence is inexcusable.”

The criticism was bipartisan. Senator Mark W. Warner, Democrat of Virginia, also called on Ms. Archuleta to step down.

“The technological and security failures at the Office of Personnel Management predate this director’s term, but Director Archuleta’s slow and uneven response has not inspired confidence that she is the right person to manage OPM through this crisis,” Mr. Warner said in a statement.

That attackers were able to compromise the agency using a contractor’s credentials is unacceptable, security experts say, given the wide availability of two-factor authentication tools, which have become standard practice, particularly since a cyberattack at Target nearly two years ago, when hackers

managed to break into the retailer's system using the credentials of a heating and cooling contractor.

"A second offense is more unacceptable than the first," said Suni Munshani, the chief executive of Protegrity, a data security company. "The O.P.M. and government agencies need to get their act together and better protect the information of their employees and citizens."

Michael D. Shear and Michael S. Schmidt contributed reporting from Washington, and Nicole Perlroth from San Francisco.

A version of this article appears in print on July 10, 2015, on page A1 of the New York edition with the headline: Hacking Exposed 21 Million in U.S., Government Says.
