The New York Times | http://nyti.ms/1KHE6r1

U.S.

Data Breach Linked to China Exposes Millions of U.S. Workers

By **DAVID E. SANGER and JULIE HIRSCHFELD DAVIS** JUNE 4, 2015

WASHINGTON — The Obama administration on Thursday announced what appeared to be one of the largest breaches of federal employees' data, involving at least four million current and former government workers in an intrusion that officials said apparently originated in China.

The compromised data was held by the Office of Personnel Management, which handles government security clearances and federal employee records. The breach was first detected in April, the office said, but it appears to have begun at least late last year.

The target appeared to be Social Security numbers and other "personal identifying information," but it was unclear whether the attack was related to commercial gain or espionage. The announcement of the intrusion came on the same day The New York Times reported that the National Security Agency had expanded warrantless surveillance of foreign hackers, an effort that could sweep up the information of innocent Americans.

There seemed to be little doubt among federal officials that the attack was launched from China, but it was unclear whether it might have been state sponsored. The administration did not publicly identify Chinese hackers as the culprits because it is difficult to definitively attribute the source of cyberattacks and to back up such an attribution without divulging classified data.

The breach is the third major foreign intrusion into an important federal computer system in the past year. Last year, the White House and the State Department found that their email systems had been compromised in an attack that was attributed to Russian hackers. In that case, some of President Obama's unclassified emails were apparently obtained by the intruders.

And last summer, the personnel office announced an intrusion in which hackers appeared to have targeted the files of tens of thousands of workers who had applied for top-secret security clearances.

In that case, the objective seemed clear: The information on security clearances could help identify covert agents, scientists and others with data of great interest to foreign governments. That breach also appeared to have involved Chinese hackers.

But because the breadth of the new attack was so much greater, the objective seemed less clear.

The intrusion came before the personnel office fully put into place a series of new security procedures that restricted remote access for administrators of the network and reviewed all connections to the outside world through the Internet. In acting too late, the personnel agency was not alone: The N.S.A. was also beginning to put in place new network precautions after its most delicate information was taken by Edward J. Snowden.

The Department of Homeland Security's emergency cyberteam used an antihacking system called Einstein that alerted the agency to the potential compromise of federal employee data, S. Y. Lee, a spokesman, said in a statement.

The F.B.I. said it was working with other agencies to investigate the matter. "We take all potential threats

to public and private sector systems seriously, and will continue to investigate and hold accountable those who pose a threat in cyberspace," Joshua Campbell, a spokesman, said in a statement.

The personnel office told current and former federal employees that they could request 18 months of free credit monitoring to make sure that their identities had not been stolen, and it said it was working with cybersecurity specialists to assess the effects of the breach. It was clear, however, that the scope was sweeping, potentially affecting a vast majority of the federal work force. J. David Cox Sr., the president of the American Federation of Government Employees, said he had been told that the breach might have affected "all 2.1 million current federal employees and an additional two million federal retirees and former employees."

Katherine Archuleta, the personnel agency's director, said in a statement, "Protecting our federal employee data from malicious cyberincidents is of the highest priority at O.P.M."

"We take very seriously our responsibility to secure the information stored in our systems, and in coordination with our agency partners, our experienced team is constantly identifying opportunities to further protect the data with which we are entrusted," she added.

Administration officials said they made the breach public only after confirming last month that the data had been compromised and after taking additional steps to insulate other government agencies from the intrusion. Mr. Obama has been briefed on the case, officials said.

The attack drew calls for legislation to bolster the nation's cyberdefenses. In a series of Twitter posts, Representative Adam B. Schiff of California, the senior Democrat on the Intelligence Committee, called the intrusion "shocking because Americans may expect that federal computer networks are maintained with state of the art defenses."

He said enactment of new cybersecurity measures was "perilously overdue."

While determining the source of cyberattacks is notoriously difficult, federal officials say they have

become far more skilled at it in recent years, largely because of increased monitoring of malicious software entering the United States over international networks. But the most sophisticated attacks often look as if they were initiated inside the United States, and tracking their true origin can lead down many blind paths.

Most Chinese cyberintrusions into the United States, at least until recently, were aimed at the theft of intellectual property, rather than at sweeping up vast amounts of personal data.

One senior federal official said it was not clear what the Chinese government would want from personnel databases. But if the attribution to China holds, it poses an additional challenge to the Obama administration. For the past three years, Mr. Obama has been trying to move the subject of cyberattacks to the center of the American-Chinese relationship. He has spent hours discussing the subject with Xi Jinping, the Chinese president.

A year ago, the Justice Department indicted five members of Unit 61398, a hacking unit of the Chinese People's Liberation Army, accusing them of stealing data from American firms to benefit state-owned Chinese companies.

But rather than change Chinese behavior, the indictments shut down many of the formal and informal discussions between the United States and China. Chinese officials have often said that they, too, are the victims of hackers.

An annual "Strategic and Economic Dialogue" with Chinese officials is scheduled to take place this month, and cyberissues will again be in the forefront.

Correction: June 4, 2015

Because of an editing error, an earlier version of a summary with this article said incorrectly that the federal employees affected by the data breach worked for the Office of Personnel Management. The breach affected workers whose information was held by the Office of Personnel Management.

A version of this article appears in print on June 5, 2015, on page A1 of the New York edition with the headline: Data Breach Tied to

China Hits Millions .
