Officials say deeply personal information in hackers' hands

June 13 2015, byKen Dilanian And Ted Bridis

In this June 5, 2015, file photo, a gate leading to the Homeland Security Department headquarters in northwest Washington. Hackers stole personnel data and Social Security numbers for every federal employee, a government worker union said Thursday, June 11, 2015, charging that the cyberattack on U.S. employee data is far worse than the Obama administration has acknowledged. (AP Photo/Susan Walsh, File)

Deeply personal information submitted by U.S. intelligence and military personnel for security clearances—mental illnesses, drug and alcohol

use, past arrests, bankruptcies and more—is in the hands of hackers linked to China, officials say.

In describing a cyberbreach of federal records dramatically worse than first acknowledged, authorities point to Standard Form 86, which applicants are required to complete. Applicants also must list contacts and relatives, potentially exposing any foreign relatives of U.S. intelligence employees to coercion. Both the applicant's Social Security number and that of his or her cohabitant are required.

In a statement, the White House said that on June 8, investigators concluded there was "a high degree of confidence that ... systems containing information related to the background investigations of current, former and prospective federal government employees, and those for whom a federal background investigation was conducted, may have been exfiltrated."

"This tells the Chinese the identities of almost everybody who has got a United States security clearance," said Joel Brenner, a former top U.S. counterintelligence official. "That makes it very hard for any of those people to function as an intelligence officer. The database also tells the Chinese an enormous amount of information about almost everyone with a security clearance. That's a gold mine. It helps you approach and recruit spies."

The Office of Personnel Management, which was the target of the hack, did not respond to requests for comment. OPM spokesman Samuel Schumach and Jackie Koszczuk, the director of communications, have consistently said there was no evidence that security clearance information had been compromised.

The White House statement said the hack into the security clearance database was separate from the breach of federal personnel data

announced last week—a breach that is itself appearing far worse than first believed. It could not be learned whether the security database breach happened when an OPM contractor was hacked in 2013, an attack that was discovered last year. Members of Congress received classified briefings about that breach in September, but there was no public mention of security clearance information being exposed.

Nearly all of the millions of security clearance holders, including some CIA, National Security Agency and military special operations personnel, are potentially exposed in the security clearance breach, the officials said. More than 4 million people had been investigated for a security clearance as of October 2014, according to government records.

Regarding the hack of standard personnel records announced last week, two people briefed on the investigation disclosed Friday that as many as 14 million current and former civilian U.S. government employees have had their information exposed to hackers, a far higher figure than the 4 million the Obama administration initially disclosed.

American officials have said that cybertheft originated in China and that they suspect espionage by the Chinese government, which has denied any involvement.

The newer estimate puts the number of compromised records between 9 million and 14 million going back to the 1980s, said one congressional official and one former U.S. official, who spoke to The Associated Press on condition of anonymity because information disclosed in the confidential briefings includes classified details of the investigation.

There are about 2.6 million executive branch civilians, so the majority of the records exposed relate to former employees. Contractor information also has been stolen, officials said. The data in the hack revealed last week include the records of most federal civilian employees, though not

members of Congress and their staffs, members of the military or staff of the intelligence agencies.

On Thursday, a major union said it believes the hackers stole Social Security numbers, military records and veterans' status information, addresses, birth dates, job and pay histories; health insurance, life insurance and pension information; and age, gender and race data.

The personnel records would provide a foreign government an extraordinary roadmap to blackmail, impersonate or otherwise exploit federal employees in an effort to gain access to U.S. secrets —or entry into government computer networks.

Outside experts were pointing to the breaches as a blistering indictment of the U.S. government's ability to secure its own data two years after a National Security Agency contractor, Edward Snowden, was able to steal tens of thousands of the agency's most sensitive documents.

After the Snowden revelations about government surveillance, it became more difficult for the federal government to hire talented younger people into sensitive jobs, particularly at intelligence agencies, said Evan Lesser, managing director of ClearanceJobs.com, a website that matches security-clearance holders to available slots.

"Now, if you get a job with the government, your own personal information may not be secure," he said. "This is going to multiply the government's hiring problems many times."

The Social Security numbers were not encrypted, the American Federation of Government Employees said, calling that "an abysmal failure on the part of the agency to guard data that has been entrusted to it by the federal workforce."

"Unencrypted information of this kind this is disgraceful—it really is disgraceful," Brenner said. "We've had wakeup calls now for 20 years or more, and we keep hitting the snooze button."

The OPM's Schumach would not address how the data was protected or specifics of the information that might have been compromised, but said, "Today's adversaries are sophisticated enough that encryption alone does not guarantee protection." OPM is nonetheless increasing its use of encryption, he said.

The Obama administration had acknowledged that up to 4.2 million current and former employees whose information resides in the Office of Personnel Management server are affected by the December cyberbreach, but it had been vague about exactly what was taken.

J. David Cox, president of the American Federation of Government Employees, said in a letter Thursday to OPM director Katherine Archuleta that based on incomplete information OPM provided to the union, "the hackers are now in possession of all personnel data for every federal employee, every federal retiree and up to 1 million former federal employees."

Another federal employee group, the National Active and Retired Federal Employees Association, said Friday that "at this point, we believe AFGE's assessment of the breach is overstated." It called on the OPM to provide more information.

Former Rep. Mike Rogers, one-time chairman of the House Intelligence Committee, said last week that he believes China will use the recently stolen information for "the mother of all spear-phishing attacks."

Spear-phishing is a technique under which hackers send emails designed to appear legitimate so that users open them and load spyware onto their

networks.