More data hacks could emerge from probe: US officials

June 16 2015, by Rob Lever

Following disclosures of devastating breaches of US government computer networks, officials from the Office of Personnel Management told lawmakers even more intrusions may be discovered with investigations and deployment of new security tools

Following disclosures of devastating breaches of US government computer networks, officials told lawmakers Tuesday even more

intrusions may be discovered with investigations and deployment of new security tools.

At a congressional hearing where lawmakers voiced outrage over the hacking incidents, the head of the Office of Personnel Management warned that more bad news may be coming.

OPM chief Katherine Archuleta did not mention China—which has been widely blamed for the incidents—but told the hearing that "these adversaries are sophisticated, well funded and focused. These attacks will not stop. If anything, they will increase."

Archuleta said that without recently implemented security measures "we would have never known that malicious activity had previously existed on the network, and would not have been able to share that information."

Andy Ozment, an assistant security at the Department of Homeland Security, also warned of more incidents.

"As our detection methods continue to improve, more events will come to light," he said.

The agency indicated in early June that some four million current or former government employees were hit. Later reports said the breach may have affected all federal employees as well as contractors and retirees, and could include sensitive data from background investigations.

Archuleta said that "there is a high degree of confidence that systems related to background investigations ... may have been exfiltrated."

'It's unacceptable'

As the hearing opened, lawmakers berated the government for failing to heed repeated warnings about weaknesses in computer networks over the past few years.

House Oversight and Government Reform Committee Chairman Jason Chaffetz, pictured on June 3, 2015, berated the government for failing to heed repeated warnings about weaknesses in computer networks

"This has been going on for years and it's unacceptable," House government oversight committee chairman Jason Chaffetz said.

Chaffetz said vulnerabilities were highlighted in several internal reports and that failure to act was "akin to leaving all the doors and windows of your house open."

Chaffetz said inspector general reports dating back to 2007 identified these problems.

"For any agency to consciously disregard its data security for so long is grossly negligent," he said.

Representative William Hurd said the incident is "another reminder of the undeniable fact that America is under constant attack... our enemies are attempting to rob our people on a daily basis."

OPM has said it has identified at least two separate intrusions and was working with the FBI and other law enforcement agencies on investigating the incidents.

Pressed abut the number of people affected, Archuleta said the first incident was "approximately 4.2 million" but that she could not confirm reports that as many as 14 million employee records were hit.

"We are working with the (relevant government) agencies to determine how many of their employees were affected," she said.

"We do not have that number at this time but we will get back to you."

In a heated exchange with Chaffetz, Archuleta declined to discuss details about sensitive data stolen, saying she would disclose that in a classified hearing.

Chaffetz berated the official for failing for heed inspector general's reports.

"They recommended it was so bad you should shut it down and you didn't and I want to know why," he said.

Donna Seymour, the chief information officer at OPM, said a more secure system with "new architecture" and encryption is being implemented but that it takes time to deal with decades of data.

"Some of our legacy systems are not capable of accepting that encryption," Seymour said.

Several security analysts have said the hack likely part of an effort by Chinese intelligence for long-term profiling—and possibly more nefarious things.

Considerable evidence points to China, suggesting long and patient efforts in Beijing to collect and compile data which may be useful in the future, according to security analysts.