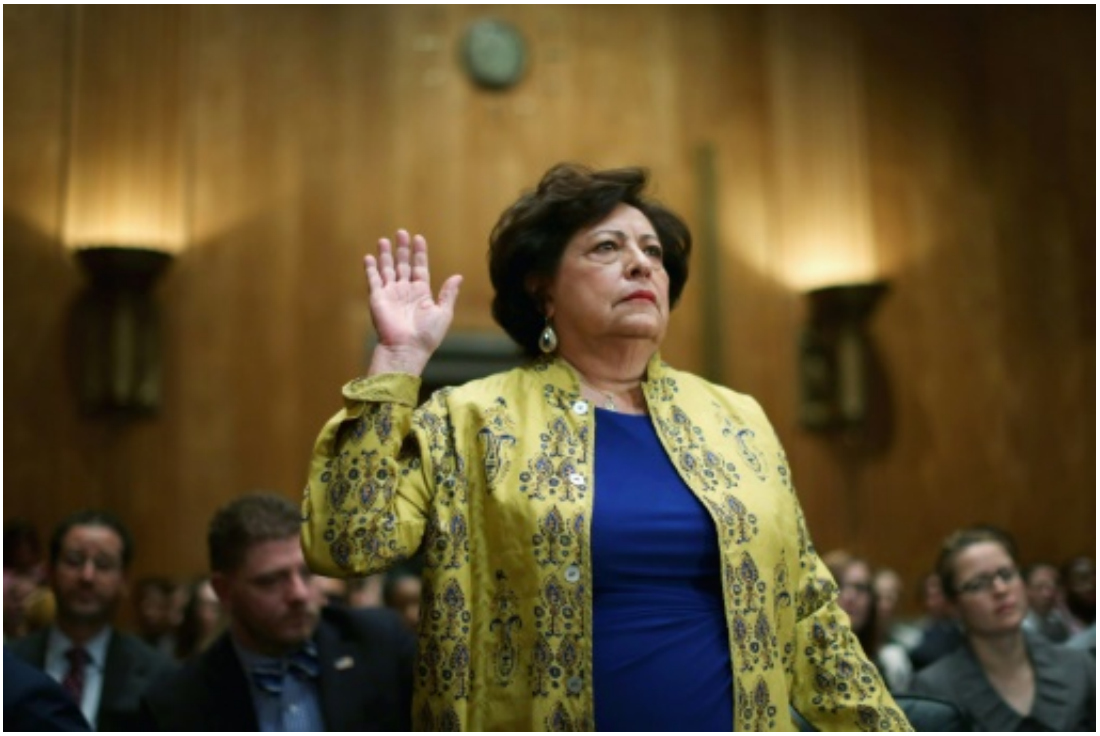
Top US official quits after massive government hack

July 10 2015, by Rob Lever



Katherine Archuleta came under criticism after revelations that the hack, which many suspect originated in China, affected a staggering 21.5 million people, far more than initially believed

The director of the US Office of Personnel Management resigned Friday after a devastating hack of government databases that saw the personal information of millions of federal workers and contractors stolen.

Katherine Archuleta had come under criticism after revelations that the hack, which many suspect originated in China, affected a staggering 21.5 million people, far more than initially believed.

The data breach swept up Social Security numbers and other information about current and former government workers, applicants, contractors and spouses of those who underwent background checks for security clearances.

"I conveyed to the president that I believe it is best for me to step aside and allow new leadership to step in, enabling the agency to move beyond the current challenges," said Archuleta, who had been in the post since November 2013.

A White House official said President Barack Obama had "accepted her resignation and thanked her for her years of dedicated service."

Beth Cobert will from Saturday assume the role of acting OPM director, the official said.

Outrage has been growing in Washington and among federal workers over the breach, an incident which puts officials in a quandary over dealing with China, the main suspect in the attack. Beijing insists it had nothing to do with the hack.

Democratic US Senator Barbara Mikulski called the hack "as outrageous and unacceptable as it is devastating."

"This erodes confidence going forward that the federal government will be able to protect federal employees," she said.

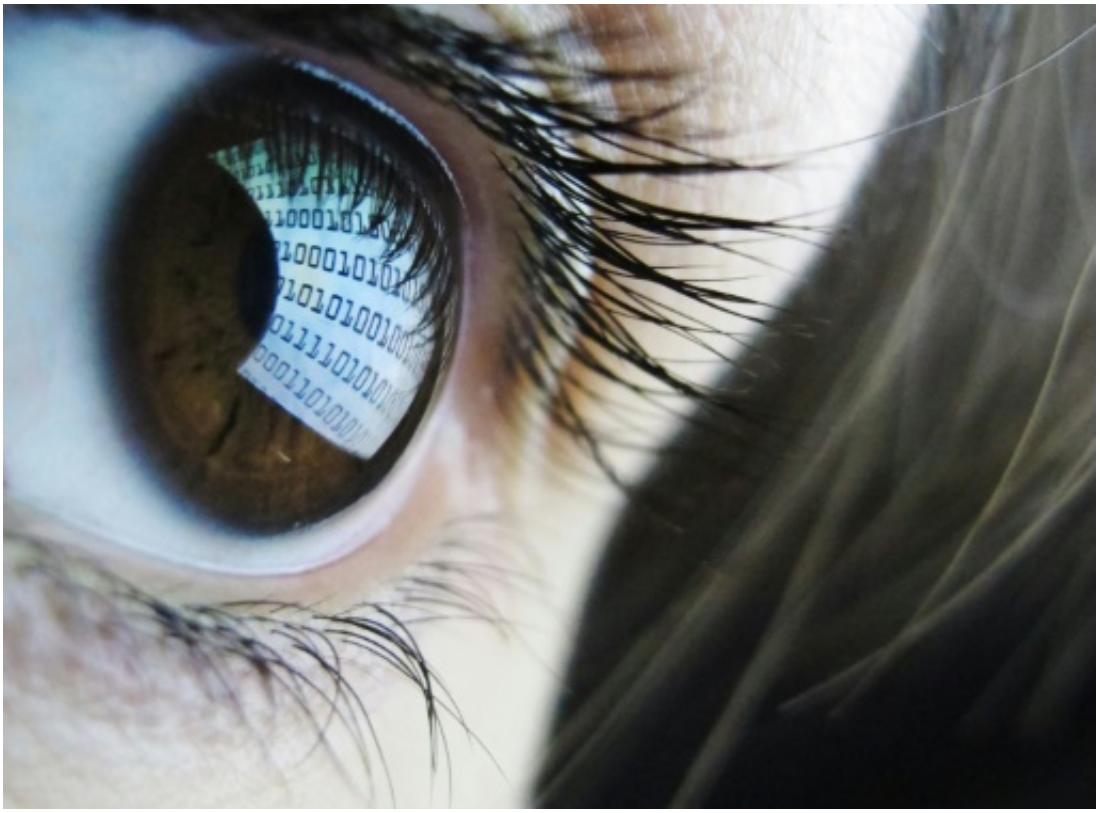
The results of an investigation released Thursday show hackers accessed personal, financial and health data, in addition to fingerprints of some

and information about spouses and cohabitants of employees.

The National Treasury Employees Union, which has sued over the breach, said the government's offer of three years of fraud monitoring was woefully inadequate.

The union "continues to be outraged that so many of our members have had their personal information compromised due to these breaches," union president Colleen Kelley said.

"We will continue to pursue our lawsuit to provide lifetime credit monitoring and identity theft protection."



Outrage has grown over the massive hack of the US government, an incident which puts Washington in a quandary over dealing with China, the main suspect in the attack

Total 22.1 million affected

An update from the OPM said those affected were 19.7 million who underwent a background investigation, and 1.8 million others, mostly spouses or cohabitants of applicants for government jobs.

Officials last month said 4.2 million personnel records were breached in a separate but related attack affecting current, former and prospective federal employees.

Taking into account overlap between the two groups, a total of 22.1 million people were affected, officials say.

The breach prompted a series of congressional hearings and widespread criticism of America's cyber defenses.

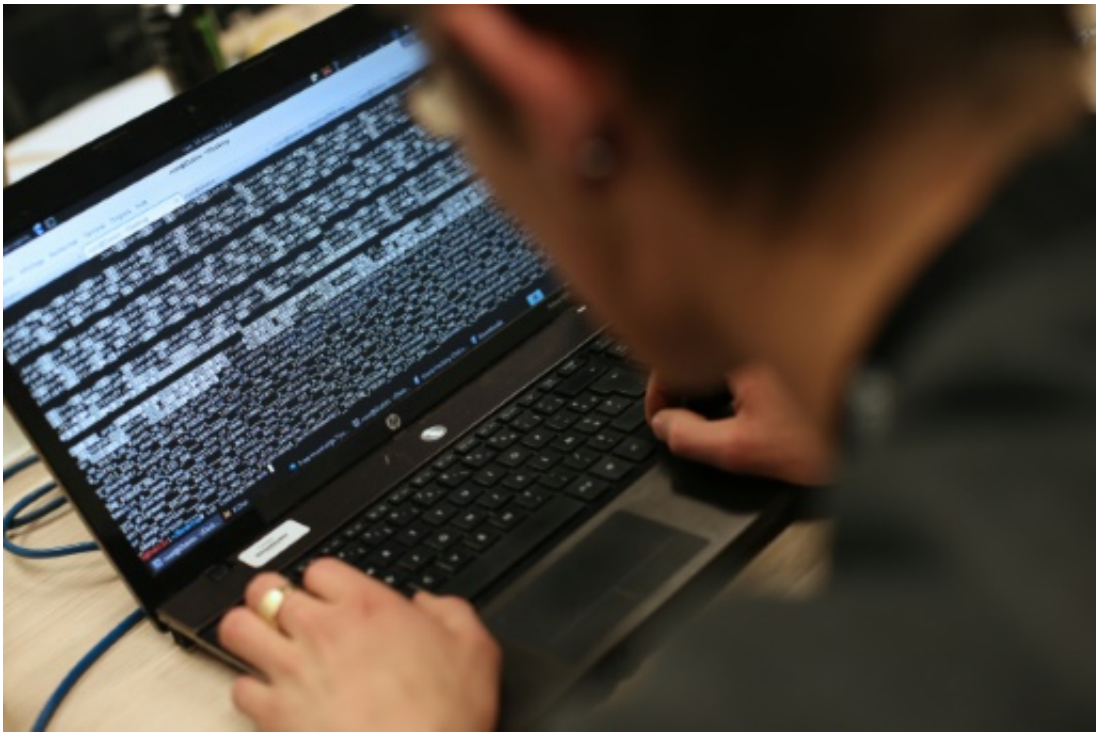
An OPM statement noted that for anyone who underwent a background investigation in 2000 or later, "it is highly likely that the individual is impacted by this cyber breach."

Republican House Speaker John Boehner had earlier called for Archuleta to be fired.

"It has taken this administration entirely too long to come to grips with the magnitude of this security breach," Boehner said in a statement.

"I have no confidence that the current leadership at OPM is able to take on the enormous task of repairing our national security. Too much trust has been lost, and too much damage has been done."

China under scrutiny



Hackers who breached US government databases stole personal information of 21.5 million people, officials said

Officials declined to comment on the assertion that China was behind the massive breach, even though intelligence chief James Clapper said last month that Beijing was "the leading suspect."

Michael Daniel, cybersecurity coordinator at the White House National Security Council, said that "just because we are not doing public attribution does not mean we are not taking steps to deal with this."

James Lewis, a senior fellow at the Center for Strategic and International Studies, said the breach creates a host of political and diplomatic problems for the US government.

"Why the reluctance to name China? It sends a powerful message to the Chinese if we don't confront them over this, a message that they can get away with almost anything since the Americans value trade deals above security," Lewis told AFP.

Lewis added that the breach may call into question a law that prevents the National Security Agency from protecting civilian agencies.

Director of National Intelligence James Clapper said last month that Beijing was "the leading suspect" behind the massive breach

"Agencies protected by NSA didn't lose any sensitive data. Maybe it's time to change this 1987 law," he said.

Some private-sector analysts have cited evidence pointing to China and

have said the breach appears to be part of a wide-ranging intelligence operation that could gather sensitive data for recruitment, blackmail or extortion.

A Chinese foreign ministry official reiterated Beijing's denial of involvement on Friday.

"All parties should adopt a constructive attitude on this issue," the spokeswoman said.

"It is imperative to stop groundless accusations, step up consultations to formulate an international code of conduct in cyberspace... in the spirit of mutual respect."