5-ABC News-OPM

OPM's chief information officer, Donna Seymour, called the matter "grave and serious."

And a top Homeland Security official said he is "deeply concerned." *[Worry]*

U.S. officials publicly acknowledge 4.2 million current and former federal employees may have had their personal information compromised when personnel records were breached in the attack. And officials now concede information tied to background investigations of current, former and even prospective employees may have been compromised.

But those officials testifying today declined to say how many people could be impacted by the theft of background-investigation information *[Deny]* â€“ even as it becomes increasingly clear the cyber-attack may have exposed sensitive information of U.S. military, law enforcement, diplomatic and intelligence officials around the world, including "foreign contacts" and relatives living overseas.

Nevertheless, the officials did offer some new insight into how hackers, believed to be from China , were able to access OPM's systems.

The DHS official, Assistant Secretary Andy Ozment, said the hackers obtained a valid user's "credentials" — such as log-in information — to enter OPM's vast network.

On Friday, ABC News reported that the OPM hackers may have used information stolen last year from a private government contractor, KeyPoint Government Solutions, to ultimately break into federal systems.

Authorities suspect hackers were able to extract electronic credentials or other information from within KeyPoint's systems and somehow use them to help unlock OPM's systems, sources briefed on the matter told ABC News.

KeyPoint representatives contacted by ABC News on Friday declined comment. And officials asked about the possible link at today's hearing wouldn't respond publicly *[Deny]*.