



Congress of the United States
House of Representatives
Washington, DC 20515

June 17, 2015

Katherine Archuleta
Director of the United States Office of Personnel Management
U.S. Office of Personnel Management
1900 E Street, NW
Room 5H09
Washington, DC 20415-1000

Dear Ms. Archuleta,

We are all justifiably alarmed that the Office of Personnel Management (OPM) has been subject to a major cyberattack that compromised the privacy of millions of current and former federal employees including contactors. I and many of my constituents have already been sent letters alerting us to this breach of our personal information that has been "compromised." As you know, these cyberthieves stole personal data such as Social Security numbers, as well as background investigations on federal employees, contractors, and applicants.

What is most alarming about this most recent criminal hack is that it was launched less than 18 months after a previous severe network assault on OPM. The trust between our federal employees, our citizens, and their government's capability to thwart an attack is without a doubt damaged. Serious security measures to avoid these lapses need to be crafted and put in place in advance of the next attack. We owe this to all our federal government employees and senior government officials who disclose very sensitive and personal information when they receive their security clearances.

I would like a personal briefing from OPM on how and why this cyberattack occurred and the steps that you have instituted, if any, to prevent a future attack. I would also like to know how many of my constituents in Virginia's 10th Congressional District are affected by this latest breach. Identity theft, especially by a potential foreign entity, is a very serious national security issue that touches many of my constituents' lives.

Sincerely,

A handwritten signature in blue ink that reads "Barbara".

Barbara Comstock
Member of Congress