Published on *The National Law Review* https://natlawreview.com

OPM Data Breach (cont'd): What We Know Now and What Questions Remain

Article By:

Michael D. Maloney

Charles R. Lucy

On July 10, 2015, U.S. Office of Personnel Management Director Katherine Archuleta resigned her post. Her departure was rather abrupt, coming just hours after her statements indicating that she would not resign. Her departure also came just hours after the true scope of the OPM data breach emerged. This is a good time for government contractors to review what we know about the OPM data breach and what questions remain.

What Was the Scope of the Data Breach?

Original estimates from OPM pegged the scope at 3 or 4 million. Upon further review, it appears that records of more than 21.5 million federal employees and contractors were stolen. It has been said that every background investigation form completed by OPM since 2000 was taken. By any measure, this OPM cyber intrusion was massive.

What Happened?

Archuleta testified that the data breach resulted from theft of a background check contractor's credentials. Sounds familiar, right? So far, no one is saying that contractor did anything wrong.

It also appears that the OPM breach was actually multiple data breaches. According to Congressional testimony from Dr. Andy Ozment, DHS Assistant Secretary for Cybersecurity and Communications, a Department of Interior data center that housed OPM records was the subject of one cyberattack that ran from October 2014 until March 2015. That hack involved approximately 4.2 million federal personnel records. A separate data breach on OPM's network involved several OPM applications related to background investigations and ran from June 2014 until January 2015. That data breach involved more than 21.5 million individuals' records.

Who's to Blame?

Certainly, OPM chief Archuleta bears some responsibility for the attacks. OPM had been warned repeatedly that its systems were outdated and vulnerable. But that's an old story that is all too

common throughout the federal government. In fact, according to a Government Accountability Office (GAO) report, 19 of 24 federal agencies have declared cybersecurity as a "significant deficiency or material weakness." Ironically, without Director Archuleta's efforts, OPM may not have discovered the breach (at least according to her July 4, 2015 message).

Although there has been no official announcement, unofficial sources have pointed to Chinese hackers as the likely culprits.

What's Next?

Victims of the cyber-attack will receive credit monitoring and identity theft protection. There is even talk that those benefits will be extended to all federal workers.

OPM announced that its on-line background investigation system, E-QIP will be shut down while security upgrades are installed. The system is expected to be down for 4 to 6 weeks. OPM uses that system to process background checks on contractors. If that system is shut down, there will be delays in contractors' security clearances. Those delays could impact contract performance.

OPM's interim director, Beth Cobert is left to clean up this mess for now while the Obama administration searches for a permanent director. Given the current status—and with proper funding—we are confident that OPM's systems will be improved.

Is the OPM data breach just the tip of the iceberg? Congress has already asked that question. Only time will tell.

GAO and others have called for improved security for government IT systems for some time. That clarion call has included a recommendation for implementing two-factor authentication. In fact, OPM's Inspector General recommended two-factor authentication in his FY 2014 audit report. But would those measures have made a difference here? At a minimum, two-factor authentication would have made it harder for the hackers to obtain the credentials in the first instance. And maybe that would have been the end of the matter. The federal government and its contractors have numerous other security protocols at their disposal. Those should be implemented rapidly to protect the country's sensitive data. Otherwise, more data breaches like the OPM data breach are inevitable.

National Law Review, Volume V, Number 201