Chairman Jason Chaffetz
Opening Statement
"OPM Data Breach: Part II"
Wednesday, June 24, 2015

As we come together here today, a lot of questions remain about what happened last month when the Office of Personnel Management discovered one of the biggest data breaches in our country's history.

That uncertainty is unacceptable.

The most recent public reports indicate that many more Americans were affected by the breach than originally disclosed.

Federal workers and their families deserve answers on both the scope of the breach and the types of personal information compromised.

Because of these many outstanding questions, we still don't understand the extent to which this breach threatens our national security.

However, according to the Intelligence Community, the risk is significant.

Only the imagination limits what a foreign adversary could do with detailed information about a federal employee's education, career, health, family, friends, neighbors, and personal habits.

OPM is currently attempting to overhaul its technical infrastructure, but without a full understanding of the scope or the cost of the project.

In fact, the agency kept the project from the Inspector General for over a year.

The IG determined OPM's Chief Information Officer "initiated this project without a complete understanding of the scope of OPM's existing technical infrastructure or the scale and cost of the effort required to mitigate it to the new environment."

Because of these concerns, the project is "possibly making [the OPM] environment less secure, and increasing costs to taxpayers."

The IG also raised questions about why OPM awarded a sole source contract for this project without going through the process for full and open competition.

It certainly seems like OPM is hastily trying to board up the house well after the hurricane has destroyed it.

We left the last hearing with more questions than answers.

I understand the agency is still investigating what happened and some of the information is going to be classified.

The classified briefing for all members last week provided little new information about the scope of the breach.

To that end, it seems like in addition to a data security problem, we have a **data management** problem.

It is unclear why so much background information related to security clearances was readily available on the OPM system to be hacked.

It is unclear to me why there is a need for SF-86 background information to be available on the network if the applicant isn't **currently** being investigated.

If information isn't accessible on the network, it can't be hacked.

So if a security clearance isn't under investigation, wall off the data.

We have to do a better job of anticipating our adversaries and protecting information we from unnecessary exposure.

Yesterday, Ms. Archuleta stated no one is personally responsible for the OPM data breach and instead blamed the hackers.

I disagree.

As the head of the agency, Ms. Archuleta is—in fact—**statutorily** responsible for the security of the OPM network and managing any related risk.