Opening Statement
Chairman Jason Chaffetz
OPM: Data Breach
June 16, 2015

Last week, we learned that the United States of America may have had what may be the most devastating cyber attack in our nation's history. And that this may be happening over a long period of time.

As we sit here this morning, there is a lot of confusion about exactly what personal information for millions of current and former federal employees and workers was exposed through the latest data breach at Office of Personal Management (OPM).

OPM initially reported that the personal information of over four million federal employees was exposed during this hack. More recent public reports suggest the breach was perhaps far worse than that.

It is also unclear exactly what information was exposed. We would like know what information was exposed, over what period of time and who has this vulnerability.

The breach potentially included highly sensitive personal background information collected through security clearance applications.

The loss of this information puts our federal workforce at risk, particularly our intelligence officers and others working on sensitive projects around the globe.

While we understand some of this information will be classified and can't be discussed here this morning, we do need clear up exactly what happened and what information was compromised.

And we need to understand why the federal government – and OPM in particular – is struggling to guard some of our nation's most important information.

The fact OPM was breached should come as no surprise given its troubling track record on data security.

Each year, the Office of Inspector General reviews and rates its respective agency's compliance with Federal Information Security standards. According to the last eight years of IG reports, OPM's data security posture was akin to leaving all the doors and windows open at your house.

Since 2007, the OPM IG has rated OPM's data security as a "material weakness" because the agency had no I.T. policies or procedures.

It is unbelievable to think the agency charged with maintaining and protecting ALL personal information of almost ALL former and current federal employees would have so few information technology policies or procedures.

And this didn't change for eight years.

The IG has also noted the agency "does not maintain a comprehensive inventory of servers, databases, and network devices." You have to know what you have in order to protect it.

Not knowing is unacceptable.

The IG also found **11 out of 47 major information systems** (or 23 percent) at OPM lacked proper security authorization, meaning the security of 11 major systems was completely outdated and unknown.

Five of these 11 systems were in the office of the Chief Information Officer, Ms. Seymour, which is a horrible example to be setting as the person in charge of the agency's data security.

The IG only recently upgraded OPM to a "significant deficiency" when the agency finally made reorganization of its office of the Chief Information Officer a priority.

For any agency to consciously disregard its data security for so long is grossly negligent.

And the fact that the agency that did this is responsible for maintaining highly sensitive information on almost all federal employees is in my opinion, even the more egregious.

OPM isn't alone; a number of other agencies also suffered breaches in the past year.

This latest cyber hack comes on the heels of several data breaches across the government, including at the U.S. Postal Service; the State Department; Internal Revenue Service; Nuclear Regulatory Commission; and even the White House.

At the same time, the government is spending more and more on information technology. Last year, across the government we spent almost $80 billion on information technology, with $84 million at OPM alone. But when a nefarious actor is able to infiltrate so many of our government systems, and remain there for months undetected, we clearly aren't getting our money's worth.

OPM isn't alone to blame for this failure.

The Office of Management and Budget has the responsibility for setting standards for federal cybersecurity practices. And it's OMB's job to hold agencies accountable for complying with and enforcing those standards.

The Department of Homeland Security has been given the lead responsibility for serving as the federal government's "geek squad" to monitor day-to-day cyber security practices. But the technical tools that DHS has deployed to try to protect federal networks apparently aren't doing the job.

While DHS has developed EINSTEIN to monitor government networks, it only detects known intruders, proving completely useless in the latest OPM hack.

The status quo can't continue; we have to do better.

I appreciate our witnesses being here today, especially on short notice.

I look forward to learning what we can about the latest breach at OPM in a public setting. More importantly, we need to hear what we are going to do to prevent this from happening in the future.

###