**U.S. Senator John Boozman, Chairman**
**Subcommittee on Financial Services and General Government**
**Senate Committee on Appropriations**
**Hearing Statement**
**June 23, 2015**
**Review of Information Technology Spending and Data Security**
**at the U.S. Office of Personnel Management**

The massive breach of OPM systems may have been the most devastating cyber-attack in our nation's history. Unfortunately, while the news reports about these incidents have been shocking, they should not be surprising. The OPM incident follows several across government and is only the latest example of the federal government's inability to protect itself from cyber security threats.

Today's hearing before the Subcommittee on Financial Services and General Government is intended to elicit further information about the recent OPM data breaches. It is also a time to discuss the enormous challenges facing the federal government as it attempts to ensure this does not happen again.

The government spends approximately $82 billion annually on information technology.

Given the cost of these projects and their impact on our economy and national security, members of the subcommittee have an ongoing commitment to conducting oversight. We must ensure that hard-earned tax dollars of millions of Americans are being spent wisely and effectively.

Just last year, this subcommittee held a hearing with OPM Director Archuleta, former federal CIO Steve Van Roekel, former GSA Administrator Dan Tangherlini, and the Director of IT Management Issues at GAO, David Powner. Given the enormous resources and important security interests at stake, the Subcommittee considered it imperative that OMB and federal agencies appropriately manage these projects.

We are well aware of examples of projects that ended in spectacular failure, as with the initial rollout of Healthcare.gov. While that kind of crisis makes news, we should also be troubled by the accounts that don't grab headlines, including initiatives with ongoing costs that grow year after year without demonstrating effective results or sufficient security.

We must have safeguards in place to ensure that oversight of these projects is consistent, that problems are anticipated before they occur, and most importantly, that someone is actually accountable and responsible.

All too often large, complex IT projects drag on for years, outlasting the Administration that initiated them and the employees responsible for managing them.

In the FSGG bill alone, billions have been spent over the years on tax systems modernization at the IRS, work that has been continuing for decades and is still incomplete. Even for projects now on track, past problems generated millions in additional costs and years of delay. And as we have seen recently at IRS, and once again with the OPM breach, both of which have compromised the personal data of millions of Americans, billions of federal dollars spent are no guarantee of security.

Across the government, IT projects too frequently go over budget, fall behind schedule, and do not deliver value to taxpayers.

Responsibility for oversight is often fragmented throughout the agency owning the project, and OMB does not conduct appropriate review and management. Whether issues relate to program requirements, performance, spending or security, lots of people are involved, but often no clear lines of accountability are drawn.

What has happened at OPM is devastating. Millions of Americans and their families and friends have been affected. Giving those impacted limited free credit monitoring and identify theft insurance will not be enough to address the long-term consequences that we may see for years to come.

But also troubling is the knowledge that OPM is just the most recent example of the government's systemic failure to protect itself. According to GAO, we should have serious concerns for the future -- the number of information security incidents reported by federal agencies has exploded in recent years. Constant vigilance is required and GAO has found that government systems may not be prepared for the job.

Nineteen of 24 major federal agencies have reported deficiencies in information security controls. Inspectors general at 23 of those agencies cited information security as a major management challenge.

How many headlines of serious data breaches will it take to implement the steps necessary to protect ourselves?

And at what point do some in Washington recognize that growing the bureaucracy without actually governing is a recipe for this type of disaster?

The Obama Administration views the federal government as capable of tackling almost every problem the nation faces. Yet, while attempting to grow the size and scope of the federal government at every turn, the Administration fails to follow-thru on the tasks it is already responsible for. If you bounce from one big government solution to another--without carrying out your basic responsibilities--this is what happens.

It is easy to suggest more money is the solution. That seems to be the response the Administration leans on every time there is a problem. But it is often the wrong choice, especially in situations like this where it appears that the problem is something much greater than a lack of resources.

The American people have lost faith in their institutions. The last thing they will do is trust Washington to solve a problem when it can't even protect the personal information of those it employs. There needs to be a dramatic change in the status quo.

What I hope to hear from our witnesses today is not the same stale line that more money is needed, but an explanation as to why the federal government failed to do the basic job of protecting personal data of millions of employees with the vast resources it already has in hand,

what it is doing right now to resolve this problem and what is being done to ensure we are prepared for the next attack.

I hope with your help we can learn from this incident and identify ways to improve our security.

I appreciate the interest of all of my colleagues and our shared commitment to doing what we can to work together to try to address this issue.  We cannot afford not to.

Senator Coons.