OPENING STATEMENT

Ranking Member Don Beyer (D-VA)
Subcommittee on Oversight
Committee on Science, Space & Technology

Is the OPM Data Breach the Tip of the Iceberg?
Joint Subcommittee Hearing

July 8, 2015

Thank you Chairs Comstock and Loudermilk for holding this hearing today. I believe this is an important hearing and I look forward to hearing from our witnesses. I believe this is an important and timely hearing. Earlier today it was reported that the New York Stock Exchange, United Airlines and Wall Street Journal are all suffering from a "computer glitch" that has disrupted their computer networks. Whether this event is determined to be intentional or not it highlights the potential vulnerability of our digital dependence. Today's hearing, however, is about another computer incident at the Office of Personnel Management or OPM.

Deterring, detecting and defending against the multitude of on-line threats that constantly lurk in the cyberspace domain is a critical issue for the federal government and private sector alike. Last year alone federal agencies reported nearly 70,000 individual computer security incidents to the U.S. Computer Emergency Readiness Team or CERT. During the same time period, from October 1, 2013 to September 30, 2014, non-Federal entities reported more than 570,000 incidents and many other incidents are potentially not identified and others not reported at all.

Cyber threats are constant and evolving, some are very sophisticated and many pose serious distress to companies, agencies and individuals. The two recent data breaches of the Office of Personnel Management (OPM) are particularly important to me and my constituents. Representing a congressional district just outside the nation's Capital many of my constituents are federal employees who may have had their personal data compromised as a result of these intrusions. One of those attacks is believed to have compromised the personal information of more than 4 million individuals and the other is suspected to have compromised the data of as many as 14 million people. I am particularly troubled that the data that was reportedly accessed included not just the personnel files but the security files of our defense, homeland security and intelligence community employees. This could potentially jeopardize their financial security, personal safety and ultimately the secrets they are entrusted to help protect for our Nation.

While the facts of this case are still being unraveled, including the motive for the attack, the identities of the perpetrators and the potential damage they may have caused, we should understand too that the federal government is not alone in being victim to cyberattacks. In the past year, hundreds of millions of personal records have been compromised by hackers targeting JP Morgan Chase, Ebay, Home Depot and other private companies.

Still, the OPM breach was significant. I am concerned for the personal and professional impact of this breach on our dedicated federal workforce, particularly those involved in the national security arena. It should not be understated the impact this has on the morale of a workforce that has recently endured – through no fault of their own – a government shutdown, forced furloughs, staffing cuts, and pay freezes. These government employees now have the added insult of a breach of their personal data.

Agency heads should also be mindful and accommodating of impacted federal employees who need time off to mitigate the fallout from the hack. I encourage OPM to communicate with all agencies to ensure workers are accommodated so that they can visit their banks, Social Security offices, and creditors in order to deal with the repercussions of the breach.

I am also concerned that reports of this attack suggest it may have been the result of individuals with ties to foreign entities and I am concerned that it appears a private company working for the government as a security contractor may have been the weak link in the chain of events that ultimately led to a successful attack.

The Federal government is making steady, but slow progress in fortifying our cyber defenses from potential attack.   According to the Office of Management and Budget's (OMB's) annual report on the Federal Information Security Management Act (FISMA) sent to Congress in February there has been improvement in federal agencies implementing continuous monitoring of their networks and the authentication of their users, for instance. But the results are still not good enough. Federal Agencies need to do a better job meeting the IT security criteria demanded by compliance with FISMA and they need to apply the cyber security standards recommended by the National Institute of Standards and Technology (NIST) to their networks. At the same time, Congress and the public need to realize that no matter how well protected an Agency or private entity is that they will never be 100-percent secure and that data breaches are bound to occur in the future.

I hope our witnesses can help provide us with advice on closing cyber-security holes when and where they exist and augmenting our security defenses against them.

With that I yield back.