OPENING STATEMENT

Ranking Member Don Beyer

House Committee on Science, Space, and Technology
Subcommittee on Environment
Subcommittee on Oversight
"Cyber Security: What the Federal Government Can Learn from the Private Sector"
January 8, 2016

Thank you Chairwoman Comstock and Chairman Loudermilk for holding today's hearing.

As we all know, and unfortunately keep relearning after each new attack, cybersecurity is a critical and daunting challenge. Today the data we create, store, access, and often share online contains information about almost every aspect of our lives. Our collective digital universe is composed of banking records, birth records, personal health files, government records, including tax filings and for some government workers, sensitive security background information. Communication that once happened in person or by phone is now online. We electronically communicate with our children's teachers about their academic achievements and social needs, and interact on a multitude of different digital social media platforms with our friends, family and colleagues. This should not come as a shock or news flash to anyone, but none of this information is fully secure.

Immediate access to these digital connections provides tremendous advantages for businesses and consumers, government agencies, educators and students, scientists, researchers, physicians and security analysts. But it also offers abundant nefarious opportunities for cyber criminals, foreign governments intent on cyber espionage, and other perhaps even more dangerous actors. Protecting against known and emerging cyber threats is an ongoing enterprise that requires consistent vigilance and continuing adoption of new operational methods and innovative technologies to thwart these escalating criminal activities and dangerous hazards in cyberspace.

Last year's announcement that the Office of Personnel Management - or OPM - suffered a major cyberattack was deeply concerning for having exposed the records of millions of records of federal workers. There were management and procedural failures at OPM that are now being addressed. But nobody is immune from cyber-attacks, not in the government and not in the private sector.

According to Privacy Rights Clearinghouse, a nonprofit, nonpartisan, organization that tracks cyberattacks, in 2015 there were 17 reported breaches against .gov or .mil addresses that resulted in access to 27.8 million records. During the same time period, the private sector, including commercial businesses, healthcare providers, and universities experienced 184 confirmed breaches that resulted in exposure of 131.5 million records.

I believe that sharing best practices to reduce IT vulnerabilities and educate federal workers, corporate employees, and consumers about the risks and threats of various cyber attacks' is an important endeavor. The point of today's hearing is to discuss what the government may be able to learn from the private sector. I am sure there are many lessons the private sector can offer the federal government and I look forward to hearing such recommendations from today's expert panel. However, I am equally certain that the federal government and its hard working IT workers and cybersecurity experts have expertise they can provide to the private sector to help improve their own security. The way I see it, this needs to be a partnership.

I look forward to discussing the importance of applying cybersecurity best practices and implementing innovative technologies at both our federal agencies and in the private sector with our witnesses today. I hope this is the first of many discussions on how we can work together to address critical cyber security issues as they expand and evolve in the future.

With that I yield back.