OPENING STATEMENT

Ranking Member Don Beyer (D-VA)
of the Subcommittee on Oversight

Committee on Science, Space, and Technology
Subcommittee on Oversight
Subcommittee on Research and Technology
"Bolstering the Government's Cybersecurity: Lessons Learned from WannaCry,"
June 15, 2017

Thank you Chairman LaHood and Chairman Comstock.

Cybersecurity should be a chief concern for every government, business, and private citizen.

In 2014, the Office of Personnel Management's (OPM) information security systems, and two of the systems used by OPM contractors, were breached by state-sponsored hackers, compromising the personal information of millions of Americans. That same year, hackers released the personal information of Sony Pictures executives, embarrassing e-mails between Sony Pictures employees, and even copies of then-unreleased Sony movies. In 2015, hackers also took control of the power grid in western Ukraine and shut off power for over 200,000 residents. These three quick examples show the varied and widespread effects of cybersecurity breaches.

The cybersecurity issue that was the genesis for this hearing was the WannaCry outbreak of last month. WannaCry ransomware infected over 300,000 computers worldwide, and could have been much worse. Fortunately, a "kill switch" was quickly found and deployed by an employee of Kryptos Logic—whose CEO, Mr. Neino is joining us today. We were lucky that a solution was found quickly, and we are fortunate that federal systems were resistant to WannaCry. But we know we may not be as lucky with the next threat. We must continue to strengthen our cybersecurity posture.

The May 11th Executive Order on "Strengthening the Cybersecurity of Federal Networks" seeks to build on the Obama administration's successes in the cybersecurity arena, and I am happy that this Administration, with which I disagree on most topics, has taken this next step. The Executive Order calls for a host of actions and a myriad of reports on federal cybersecurity from every government agency. Simultaneously, the Trump Administration has been slow to fill newly vacant positions in nearly every government agency. My concern is that understaffed agencies will have significant difficulty meeting the dictates of the Executive Order. I'm also concerned that proposed budget cuts across the agencies, if enacted, will make the task of strengthening the security of Federal information systems that much harder. We must insure that government has the resources and staffing to meet the need in this vital area.

The Executive Order also calls for agencies to begin using the NIST Framework for its cybersecurity efforts. NIST plays a very important role in setting cybersecurity standards that can

help thwart and impede cyber-attacks. NIST is world renowned for its expertise in standards development. Federal agencies will be well served by using the NIST Framework.

However, as a precautionary note, I believe some efforts to expand NIST's cybersecurity role beyond their current mission and expertise are well intentioned but misplaced. For example, our Committee recently debated H.R. 1224, the "NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017," which gives NIST auditing authority for all Federal civilian information systems. Currently, the Offices of Inspector General at each agency have the statutory authority, as well as the experience and expertise to conduct cybersecurity audits for their respective agencies. NIST has no such experience or expertise. I remain concerned about this proposal and I would be interested in any of our expert witnesses' thoughts on NIST's role in cybersecurity. But, regardless of where this important mission is placed, the Government must establish proper levels of staffing and resources. That financial reality must be addressed.

I look forward to hearing from all of today's witnesses about best cybersecurity practices of the federal government and ways for the government to improve its cybersecurity posture. I look forward to hearing from Gen. Gregory Touhill, former Federal CISO, about his experience in that positions and thoughts on the way forward for federal cybersecurity policy.

One final note, Bloomberg reported this week that the Russian meddling in our electoral system was far worse than what has been previously reported. According to the report, hackers attempted to delete or alter voter data, accessed software designed to be used by poll workers, and, in at least one instance, accessed a campaign finance database. These efforts did not need to change individual votes in order to influence the election, and we should take these sorts of cyber threats very seriously.

Mr. Chairman, this Committee held more than a half dozen hearings on cybersecurity issues during the last Congress, including one titled: Protecting the 2016 Elections from Cyber and Voting Machine Attacks. Given what we now know about hacking and meddling in the 2016 election, I hope that this hearing today will be followed up with a hearing to examine how we can better protect our voting systems.

Thank you Mr. Chairman. I yield back.