OPENING STATEMENT

Ranking Member Eddie Bernice Johnson (D-TX)

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

Thank you Chairman LaHood and Chairwoman Comstock.

As I have said many times on this subject before, cybersecurity is a difficult threat to confront. It is continually evolving and constantly presenting serious dangers to our personal and national security. Every time you pick up a newspaper, it is apparent that no one is safe from these threats. Cybersecurity weapons can compromise our government systems, financial systems, healthcare services, electric power grid, sensitive private information, and even our voting systems – the very lifeblood of our democracy.

Although some cybersecurity threats are highly sophisticated, backed by well-trained foreign actors and nation states, even crudely developed cyber threats can be successful because they rely on the flaws and vulnerabilities of unsuspecting human beings to help launch penetrations of digital networks.

Personal, private sector, and federal government vigilance is key to confronting this threat. A 22-year-old cybersecurity analyst employed by Kryptos Logic helped derail the recent Ransomware attack resulting from the WannaCry virus because he acted quickly. That is one lesson learned from the WannaCry attack. Another lesson is the importance of quickly implementing security patches issued by software providers. U.S. government and private sector systems were largely immune to WannaCry because our systems managers did just that.

Like many other cyber threats, the success of WannaCry was dependent on individuals inadvertently helping it infect computers and proliferate. Those who are simply users of digital technology today, which includes all of us, our children and grandchildren alike, should all heed these lessons. Empowering individuals to take appropriate precautions against the wide-range of current and emerging cyber threats and encouraging them to remain vigilant in both the work place and at home is one of our best defenses. People are critical to ensuring our cyber-security. The best technical tools in the world won't do much good when individuals mistakenly open the door to these digital dangers.

I look forward to the testimony of our witnesses. I would also like to thank retired Brigadier General Gregory Touhill for being here today. He has had a long career in cybersecurity. He was a deputy assistant secretary for cybersecurity and communications at DHS and was appointed as the first federal Computer Information Security Officer (CISO) last September, a position he left in January of this year. Gen. Touhill is currently an Adjunct Professor of Cybersecurity & Risk Management at Carnegie Mellon University.

Thank you General Touhill and all of our witnesses for testifying today.

Thank you Mr. Chairman. I yield back.