OPENING STATEMENT
Ranking Member Eddie Bernice Johnson (D-TX)

House Committee on Science, Space, and Technology
Subcommittee on Research and Technology
"Strengthening U.S. Cybersecurity Capabilities"
February 14, 2017

Thank you Chairwoman Comstock and Ranking Member Lipinski for holding this hearing on cybersecurity. And thank you to the witnesses for being here this morning. We have several new Members on the Committee, so it is valuable to start off the year with a "Cybersecurity 101" hearing. Today's panel includes four very distinguished experts from government, the private sector, and academia, and I know it will be an interesting and informative discussion.

I'm pleased Dr. Romine is able to join us this morning. Testifying before Congress so early during a transition in administrations can be challenging for any agency official. This is not a hearing specifically about NIST's role in cybersecurity, but I'm going to set some context with a few words about this very important but little known agency.

NIST plays a crucial role in both public and private sector cybersecurity, as we will hear about today. In fact, cybersecurity accounts for a significant fraction of NIST's total budget. However, it is but one of dozens of topics to which the hundreds of extraordinary scientists and engineers working at the NIST labs in Gaithersburg, Maryland and Boulder, Colorado devote their careers. NIST hosts the world leading measurement scientists, and uses that science to lead the development of technical standards for the nation. NIST scientists work closely with industry across all sectors, big and small, to advance U.S. innovation and competitiveness. And they do all of this on what amounts to a shoestring budget.

Because NIST usually exceeds expectations, there is a tendency by policymakers to ask them to do more with less. That has surely been true in the realm of cybersecurity. But I caution this Committee and the Administration not to push NIST to the breaking point. Every agency must set priorities, and there may be room even at NIST to put aside some of its work to make room for higher priority topics, including cybersecurity. I will be watching closely to ensure that that none of NIST's important work is compromised in our zeal to save a dollar here and dollar there. The costs to the nation will be much greater than the few dollars saved.

Finally, I want to bring up a troubling incident from 2013, in which the National Security Agency (NSA) secretly inserted a "back door" into a cryptographic standard being developed by NIST. There was an immediate outcry, as this sneak attack was widely recognized as a potentially slippery slope to a surveillance state. It undermined the stellar reputation and credibility of NIST in international circles and it had a negative impact on the global operations of U.S. corporations. In the aftermath of that incident, NIST implemented new procedures to reinforce transparency and integrity in their standards development process.

I want NIST to be able to consult with the intelligence agencies – such collaboration is necessary and appropriate in the realm of cybersecurity. Both NIST and the U.S. intelligence community share special cybersecurity expertise and skills that should be shared to help defend our nation against the many cybersecurity threats that confront us. However, I will be watching out for the slightest hint that such collaborations in any way compromise NIST's independence or the integrity of their work.

With that, I want to thank the witnesses again for your time and contributions to this Committee's discussion about cybersecurity, and I yield back.