OPENING STATEMENT

Ranking Member Eddie Bernice Johnson (D-TX)

House Committee on Science, Space, and Technology
"Protecting the 2016 Elections from Cyber and Voting Machine Attacks"
September 13, 2016

Thank you Mr. Chairman.

Ensuring that our elections are fair, accurate and freely accessible to ***all*** American citizens is fundamental to our democracy. Every instance of malfunctioning voting technology, and without question, every cyber-attack on our election system is significant. And all efforts to improve voting security, reliability, privacy, and access are welcome and important. I am comforted by the testimony of today's experts and many others that we are in a much better place today than we were 10 or 15 years ago.

I am deeply concerned, however, by some of the rhetoric in recent weeks that seems intended to erode public confidence in our election system. Prominent voices have suggested that the U.S. election system is riddled with fraud and somehow "rigged." Those conspiratorial allegations, like many others that have been floated in the public sphere this election cycle, are not supported by actual facts, and they threaten the election process we have relied upon for more than two centuries.

I am eager to hear from the distinguished panel today about the challenges of securing our elections system in the digital age, and what actions have been taken at the federal, state, and local levels to strengthen cybersecurity. However, given the reckless rhetoric as well as the other serious threats our elections system is facing, I want to take this opportunity to put the cybersecurity challenges in context.

The U.S. election system is complex and highly decentralized, encompassing approximately 10,000 local, county, and state election offices. Further, there are few connections between individual voting systems and the Internet, and at least 75 percent of voters will be able to verify their vote with a paper ballot this Fall. This compartmentalization and paper trail provides a strong firewall against any cyber threats.

The recently publicized attacks against voter registration rolls in Arizona and Illinois are serious, but have not resulted in any changes to voter data or to any votes. In Arizona, the cybersecurity firewalls worked to contain the threat. What I find most concerning are reports that these recent threats may be linked to Russian intelligence operations. So we must be vigilant, and I hope these incidents will lead to improved cybersecurity protocols and practices.

While security of the election system is important, voter **access** is fundamental to our democracy. Baseless allegations of widespread voter fraud have been used as an excuse to disenfranchise large numbers of minority and young voters through discriminatory voter ID restrictions. News21, a journalism program established by the Carnegie Corporation of New York and the John S. and James L. Knight Foundation, found voter impersonation fraud to be extraordinarily rare. An analysis of 2,068 alleged election-fraud cases in all 50 states from 2000 to 2012 out of 146 million registered voters identified only 10 cases of voter impersonation fraud. You don't enact laws because of 10 cases of fraud in 12 years unless you have an ulterior motive. Fortunately, the courts have seen right through the most blatantly discriminatory state laws.

In addition to the state-sanctioned voter ID laws, the Brennan Center for Justice and others have continued to document cases of voter intimidation, deliberate spreading of misinformation to keep minorities and students from voting, and other attempts to target and disenfranchise minority and young voters. These threats to tens or hundreds of thousands of eligible voters, whether orchestrated by public officials or lone trouble-makers, should be taken just as seriously as the cyber threat.

Mr. Chairman, I know my remarks have moved beyond the intended scope of this hearing. But you know well how passionate I am about this issue. It is my hope with this hearing that we can have a thoughtful discussion of the challenges and actions that have been taken related to cybersecurity and other voting technology issues, while avoiding adding to the noise and confusion surrounding these issues just 8 weeks out from a crucial election.

With that, I would like to welcome all of our witness for being here today. This is a distinguished panel, and I look forward to learning from your collective experience and expertise.

Thank you Mr. Chairman. I yield back.