OPENING STATEMENT

**Ranking Member Eddie Bernice Johnson (D-TX)**

House Committee on Science, Space, and Technology
Subcommittee on Oversight
*"Bolstering the Government's Cybersecurity: Assessing the Risk of Kaspersky Lab Products to the Federal Government"*
October 25, 2017

Thank you Chairman LaHood. Kaspersky Lab is one of the world's largest cybersecurity companies, and makes a popular anti-virus program used by 400 million users worldwide. But recent concerns by the U.S. intelligence community about close connections between Kaspersky Lab, its founder Eugene Kaspersky, and the Russian Intelligence Services have led to much greater scrutiny of its activities. This hearing is premised on examining what threat Kaspersky software poses to the federal government. However, the federal government has already pre-emptively addressed that threat. Last month, the Department of Homeland Security (DHS) issued a directive that required all federal agencies to identify any of their networks using Kaspersky Lab software, and gave those agencies a 90-day deadline to initiate a plan to remove Kaspersky Lab software from those computer systems. DHS decided that the security risk of having a Russian company embedded on federal computer networks was simply not worth it.

I have confidence in the ability of federal government agencies to eliminate Kaspersky Lab products from their respective computer systems. I am less confident, though, in our collective ability to identify and guard against cyber warfare actions from Russian state actors. Russian hackers have infiltrated some of our nation's nuclear power plants, private e-mail accounts, and state election databases. Russia, according to a publicly available Intelligence Community assessment, conducted an influence campaign in 2016 to undermine public faith in the US democratic process and to harm Hillary Clinton's chances of winning the Presidency. That intelligence assessment should be a wake-up call for all of us. We should expect attempts by foreign actors to affect future elections, using computer hacking, social media, and other means, as was done in 2016.

Mr. Chairman, prior to the 2016 Election, this Committee held a hearing to review the guidelines for protecting voting and election systems—including voter registration databases and voting machines. I believe a follow-up hearing would be appropriate to discuss protecting these same systems, in the light of last year's events, as well as examining the sophisticated influence operations conducted by Russian intelligence services to disrupt our democratic processes and damage our democracy. With the knowledge of Russian cyber warfare actions in 2016, we can have a more robust discussion on the measures hostile actors have been using against America's voting infrastructure, and we can discuss measures that need to be taken to bolster the security of our elections.

Mr. Chairman, I hope that you seriously consider holding a 2016 election security postmortem, with a focus on what the Science Committee can do to help protect the vote going forward. Thank you and I yield back the balance of my remaining time.