OPENING STATEMENT

Ranking Member Donald S. Beyer, Jr. (D-VA)
of the Subcommittee on Oversight

Committee on Science, Space & Technology
"Bolstering the Government's Cybersecurity: A Survey of Compliance with the DHS Directive"
November 14, 2017

Thank you, Chairman LaHood. Three weeks ago we held a hearing on security concerns related to the use of Kaspersky Lab software on federal computer networks. I think most Members across the aisle agreed that using the services or software of Kaspersky Lab, a Moscow-based company that reportedly has close ties to Russian intelligence services, on federal networks presents risks not worth taking. Back in September, the Department of Homeland Security also recognized this, and issued a directive to federal agencies to identify and initiate actions to remove Kaspersky Lab software from their networks.

I understand that we're holding this hearing as a follow-up to ensure that our federal agencies are complying with the DHS directive in a timely manner, which is important given the grave risks. However, it seems that in holding a second oversight hearing on ***solely*** Kaspersky Lab products, we're missing the forest for the trees. Kaspersky products are not ***the*** biggest security risk we face from Russia. As I mentioned at our last hearing, and as we saw throughout the 2016 election cycle, cybersecurity is no longer just about defending our data—it is, on a larger scale, about defending our democracy from unwanted foreign influence and disinformation campaigns.

Instead of focusing just on Kaspersky Lab software, we should be examining how enemies of democracy are using communication technologies in new, precise and powerful ways to disrupt our democratic institutions and influence the American public. We should be specifically looking into how the Russians have done just this during the 2016 U.S. Presidential Election and how we can develop tools, technologies, and public awareness to diminish similar attacks in the future. We should also examine the state of our cyber security practices in defending our critical election infrastructure from covert interference and manipulation. The House Science Committee has an important role in publicly addressing these issues. Mr. Chairman, at the last Kaspersky hearing, I requested that you hold a hearing on these larger issues, but I am asking once again today.

I am glad that at least one of our witnesses today will help put the security concerns regarding the use of Kaspersky Lab software in context and help us examine the broader Russian strategy of undermining our democratic institutions and influencing our democracy. Dr. Mark Jacobson, a professor at Georgetown University, has written frequently on the impact of Russia's influence operations against the United States in the past few years. I look forward to his testimony.

I welcome all of our witnesses to today's hearing. I am also attaching to my statement a Minority Staff Report that addresses Russia's cyber influence campaign against the U.S. This report has already been shared with the Majority staff.

Thank you, Mr. Chairman. I yield back.