OPENING STATEMENT

Ranking Member Don Beyer (D-VA)
of the Subcommittee on Oversight

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

Thank you Chairman LaHood.

Today's hearing is focused on the security risks presented by using computer software from the Russian company Kaspersky Lab, which produces anti-virus and other software. In July, the General Services Administration (GSA) removed Kaspersky Lab from its list of approved federal vendors. Last month, the Department of Homeland Security (DHS) issued a Binding Operational Directive (BOD) banning federal agencies from using any product or service offered by Kaspersky Lab, giving federal agencies until mid-December to implement that directive.

The founder of Kaspersky Lab, Eugene Kaspersky, is a software engineer educated at a KGB cryptography institute who later worked for the Russian intelligence service prior to starting Kaspersky Lab in 1997. Kaspersky software is now used by 400 million people worldwide and Eugene Kaspersky has been described as the Bill Gates of Russia. Security concerns about Kaspersky products and reported ties between Eugene Kaspersky, his company, and Russian intelligence services have been brewing within the U.S. intelligence community for years. Meanwhile, the company has vigorously argued that it has no ties to *any* government.

According to press reports, concerns about connections between Kaspersky Lab and Russian intelligence services have become more urgent in recent months. In April, the Senate Intelligence Committee asked the Director of National Intelligence and U.S. Attorney General to look into Kaspersky employees' relationship with Russian intelligence. In May, six U.S. intelligence agency directors, including the Directors of the CIA and NSA, told the Intelligence Committee that they would not be comfortable using Kaspersky products on their networks. In June, it was reported that FBI agents had interviewed U.S. based employees of Kaspersky Lab. In July, *Bloomberg Businessweek* published a story referencing internal company emails reportedly showing a close working relationship between Kaspersky Lab and Russian intelligence. Representatives from the company said the media 'misinterpreted' these e-mails.

Earlier this month, the *New York Times* reported that Israeli intelligence had themselves penetrated Kaspersky Lab's antivirus software and were able to determine that Russian government hackers were using the company's software to search for the code names of U.S. intelligence programs. The Israelis apparently discovered that a contractor to the National Security Agency (NSA), who had improperly taken classified documents home and stored them on his home computer that used Kaspersky's antivirus software, had his data compromised by these Russian hackers. This event reportedly occurred more than two years ago.

All of this has led to legitimate security concerns about the use of Kaspersky Lab software. But cybersecurity is no longer simply about defending our data from theft. It is about defending our democracy from disinformation campaigns that combine cyber assaults with influence operations that seek to manipulate the public sphere to undermine the public's trust in the media, our government, and our democracy. Russia has spread falsehoods and disinformation, seeking to sow divisions between us and confusion among us.

This is not, and should not be, a partisan issue in striving to defend our democracy against those who seek to damage it. Just last week, former President George W. Bush described these Russian assaults as quote "broad, systematic and stealthy" and warned that, "we must secure our electoral infrastructure and protect our electoral system from subversion."

Mr. Chairman, I hope we can have a future hearing where we hear from social scientists, researchers, and technical experts about the tools and technologies we can employ to help identify these evolving threats and defend against them. I hope that you will commit to that.

I look forward to hearing from all of our witnesses today and especially Sean Kanuck, who happens to be one of my constituents, and who is an expert on these topics. Mr. Kanuck was appointed the first National Intelligence Officer (NIO) for Cyber Issues in 2011 and served in that position at the National Security Council (NSC) until 2016. Prior to that he spent ten years at the Central Intelligence Agency's (CIA's) Information Operations Center. Today he joins us as the Director of Future Conflict and Cyber Security at the International Institute for Strategic Studies (IISS). Welcome Sean, and welcome to all of our witnesses.

Thank you Mr. Chairman. I yield back.