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.

Security concerns related to Kaspersky Lab products and reported ties between Eugene Kaspersky, his company, and Russian intelligence services have been brewing within the U.S. intelligence community for years. This is deeply troubling given that Kaspersky Lab – whose main product is anti-virus software – has offices in 32 countries, an estimated 270,000 corporate clients, and its software is used by approximately 400 million people worldwide. And, until just recently, the U.S. Government also used Kaspersky Lab's software.

The founder of Kaspersky Lab, Eugene Kaspersky, is a software engineer educated at a KGB cryptography institute who also worked for the Russian intelligence service before starting his software company in 1997. Eugene Kaspersky has been described as the "Bill Gates of Russia". Despite his background and the concerns of the U.S. intelligence community, the company has vigorously argued that it has no ties to any government.

Concerns about connections between Kaspersky Lab and Russian intelligence services have become more pronounced over the past year:

- In April, the Senate Intelligence Committee asked the Director of National Intelligence and U.S. Attorney General to look into Kaspersky employees' potential ties 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 that showed a close working relationship between Kaspersky Lab and Russian intelligence.

Finally, earlier this month, the New York Times reported that Israeli intelligence were able to determine that Russian government hackers have been using the company's software to search for the code names of U.S. intelligence programs. Specifically, the Israelis discovered that a contractor to the National Security Agency (NSA) had his data compromised over two years ago by these Russian hackers after he improperly took classified documents home and stored them on his home computer. Kaspersky's antivirus software had been installed on this contractor's home computer. Kaspersky Lab has repeatedly denied any affiliation with the Russian hacking, but just today, the company admitted in a blog post that it had collected the NSA files through routine malware data collection.

All of this has led to legitimate security concerns about the use of Kaspersky Lab software. I am glad that the U.S. Government has realized this: in July, the General Services Administration (GSA) removed Kaspersky Lab from its list of approved federal vendors. And, 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.

But, cybersecurity is no longer simply about defending our data from theft. It is also about defending our democracy from disinformation campaigns that combine cyber assaults with influence operations. Since the 2016 election, it has been well-established that 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 – together we should be striving to defend our democracy against those who seek to damage it.

Mr. Chairman, I hope we can also 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 – beyond traditional cybersecurity – 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.