Statement of Ranking Member Kathleen Rice (D-NY)

Subcommittee on Counterterrorism and Intelligence Joint Hearing:

"Access Denied: Keeping Adversaries Away from the Homeland Security Supply Chain"

Thursday, July 12, 2018 at 10:00 a.m.

The Department of Homeland Security has the enormous responsibility of securing the federal government's vast supply chain – particularly Information Technology – from a wide variety of foreign threats. Today, the most pressing threats come from Chinese and Russian IT companies, that until recently were used widely throughout the U.S. and by several federal agencies.

For example, last year we learned that the Russian cybersecurity company Kaspersky Lab was operating compromised anti-virus software in U.S. government computers. Despite being a long-time government vendor, the FBI had reason to believe the Kasperksy programs contained back doors that could be accessed by Russian intelligence. Thankfully, DHS acted to wipe the software from all government systems.

Additionally, Members of Congress have long been warned that the Chinese telecommunications companies Huawei and ZTE also posed risks to our national security. ZTE and Huawei are two of the world's largest telecommunications companies and were used widely in the U.S. However, the companies have close ties to the Chinese government and were believed to be possible vehicles for cyber theft and espionage.

In 2016, we imposed stiff penalties on ZTE for violating U.S. sanctions by making hundreds of shipments of telecommunications equipment made with U.S. parts to Iran, Sudan, North Korea, Syria and Cuba. After yet another breach in April, ZTE faced additional U.S. penalties, including a ban on U.S. suppliers selling equipment to ZTE. The following month both ZTE and Huawei were also banned from being sold on U.S. military bases.

These bans were not only warranted but, in my opinion, long overdue. These companies and their government clearly pose a threat to our national security and we had a responsibility to act. Unsurprisingly however, President Trump appears to have placed his own business interests above our national security. Not long after a soon-to-be Trump-branded resort in Indonesia received loans from the Chinese government, the President Tweeted a promise to save ZTE from the punishing penalties.

Just yesterday, the Trump Administration and the Chinese government signed an agreement to end the ban on U.S. exports to ZTE. The President's lack of candor and leadership on this issue, coupled with the urgent threats facing our supply chains, calls for the federal government to develop a comprehensive strategy to protect our supply chains from foreign threats.

During this hearing, I hope to learn more about what the Department of Homeland Security is doing to advance their counterintelligence programs specifically with the proposed use of Section 806 authority. I also want to know whether the White House is playing an active role in coordinating supply chain security across the federal government.

But most importantly, this committee needs to know what additional resources and supports are needed by the Supply Chain Risk Management program to carry out its mission effectively. As I understand, there are only two employees dedicated to the SCRM Program. That seems completely inadequate given the task ahead.

It is time that we finally listen to the Intelligence Community and create a comprehensive strategy to counter the mounting threats facing our supply chains.