FOR IMMEDIATE RELEASE

Statement of Ranking Member Bennie G. Thompson (D-MS)

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

Subcommittees on Counterterrorism and Intelligence and Oversight and Management Efficiency Joint Hearing

July 12, 2018

The threats to the U.S. from China and Russia are not new. For years, it has been reported that Chinese companies like ZTE and Huawei could be used to carry out cyber theft, spying, and espionage.

Last year, Kaspersky Labs demonstrated the Russian government's capability to use anti-virus products to compromise federal information and information systems, directly affecting U.S. national security.

In a letter to Mississippi's Secretary of State in September, I spoke of "an unacceptable amount of risk" to our national security posed by these products, not only to the supply chain but also to the security of our elections.

I am reiterating that concern today, especially since the threat from Russia and China to the U.S. has become more complicated and troubling in the wake of ongoing actions by President Trump.

After the blatant violation of U.S. sanctions in 2016 by ZTE and its subsequent breach this year, the Department of Defense initiated a ban on the sale of ZTE and Huawei products on military bases due to security concerns.

Despite these concerns, in May, the President took to Twitter to commit to saving ZTE and Chinese jobs days after a Trump-branded resort received a substantial loan from the Chinese government to build property in Indonesia.

This sent a clear message: the U.S. President will do business with you if you do business with him.

These policies continue to erode U.S. institutions and interests abroad, downplaying the seriousness of U.S. sanctions and national security to the global community.

The Federal Government supply chain is a target for our adversaries.

And while the threats from our adversaries are great, so is the opportunity to identify vulnerabilities and mitigate the risks.

Today, we are considering expanding DHS' authority to address supply chain risk by excluding contractors based on national security concerns.

Such authority would provide DHS with additional opportunities to mitigate supply chain risk during the acquisition phase.

The Defense Department currently has authority, known as Section 806 authority, to exclude contractors from information technology procurements if evidence of national security risk is identified and mitigation measures are not available. It has only been used this authority once.

Although the legislation is a good first step, we should consider whether refinements are necessary based on DOD's lessons learned.

Providing the authority won't address the fact that the Trump Administration lacks a coherent, government-wide strategy to adequately address the challenges we continue to face from Russia and China.

National Security experts, business associations and Members of this Committee have communicated their concerns to the administration, about the need to secure federal supply chains.

# # #

Media contact: Adam Comis at (202) 225-9978