



# COMMITTEE ON HOMELAND SECURITY

**FOR IMMEDIATE RELEASE**

**Hearing Statement of Chairman Bennie G. Thompson (D-MS)**

***Public-Private Initiatives to Secure the Supply Chain***

**October 16, 2019**

We are here today to discuss an issue critical to our national security: the information and communications technology (ICT) supply chain. Concerns about the origin components embedded in our ICT devices, such as cell phones, computers, and satellites, are nothing new. We have known that such technology produced by our adversaries could be exploited for espionage or cyberattacks for a long time. In 2012, the Senate Intelligence Committee released a damning report about the threats products from Chinese telecom companies ZTE and Huawei pose to U.S. national security interests.

Government officials had acknowledged concerns about the use of Kaspersky anti-virus software for years before the Department of Homeland Security finally directed all Federal agencies to remove it from their systems in 2017. But the rapid evolution of the global economy coupled with our increasing reliance on technology and anticipation of a new 5G cell network has resulted in much-needed momentum to address risks to our ICT supply chain.

Developing sound supply chain risk management policy is not just a whole-of-Government effort - it's an all hands on deck effort. That is why I am pleased that CISA is spearheading a critical public-private initiative to provide recommendations for assessing and managing ICT supply chain risks. Last month, the Task Force issued its Interim Report, and I congratulate the Task Force co-chairs on that accomplishment. The Interim Report identified practices and policies related to supply chain threat information sharing, whitelisting, and threat evaluation, along with associated challenges. I am eager to discuss those issues today. More importantly, I want to know how Congress can help advance the recommendations of the Task Force

I am also interested to learn about how the work of the Task Force is being leveraged by the Federal Acquisition Security Council and by the Department of Commerce as it executes its authorities under Executive Order 13873, which was seemingly targeted at China. On that note, I want to commend the Administration finally taking a concrete step to mitigate the threat Chinese firms pose to the supply chain. The Chinese government has spent years strategically investing in and promoting Chinese information and communications technology to advance its national agenda – at our expense. So I was disturbed last year when the President directed the Department of Commerce to lift the ban on ZTE buying U.S. parts, apparently to advance his trade agenda.

Our national security is not a bargaining chip, and the President cannot negotiate away policies that will secure our supply chain. Toward that end, I will continue to monitor the implementation of the Executive Order closely.

# # #

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