Statement of Subcommittee Chairman Scott Perry (R-PA)
Joint Subcommittee Hearing

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

July 12, 2018

Remarks as Prepared

Good morning. I would like to thank Chairman King for holding this hearing today and including the Oversight and Management Efficiency Subcommittee in this very important and timely discussion on the Department of Homeland Security's efforts to secure its supply chain.

In today's interconnected world, the federal government is increasingly reliant on the procurement of products and services with supply chains that originate from outside our borders. DHS is no exception. Global supply chains are integral to the Department's ability to carry out the mission of securing the homeland.

However, recent incidents involving government contractors and foreign-based suppliers like Kaspersky Lab, ZTE, and Huawei (Wah-Way) have shed light on the security risks associated with the global nature of supply chains.

Potential threats to international supply chains ranging from interference by foreign adversaries to poor product manufacturing practices present a unique and complex challenge for both DHS and national security.

To assess and counter supply chain threats, organizations employ supply chain risk management strategies, which leverage risk assessments to neutralize threats associated with the global and distributed nature of modern supply chains. Risk assessments are made by utilizing open and closed source research to allow organizations to better understand their supply chain and identify the threats specific to it. To assist the federal government in this effort, the National Institute for Standards and Technology has released government-wide best practices for agencies to use as a model for their own supply chain risk management strategies.

Agencies like DHS rely on contracts for products and services to carry out their daily operations. As such, in the case of the Department, ensuring supply chain security is intrinsic to the mission of ensuring national security.

Unfortunately, given the threat environment, I am concerned that the Department does not currently possess the sufficient tools to effectively carry out supply chain risk management. Under the regulations governing federal procurements, DHS maintains limited authorities to terminate procurement contracts for unforeseen circumstances and to bar irresponsible entities from doing

future business with the federal government for up to three years. Additionally, the Federal Information Security Modernization Act of 2014 granted the Department the authority to issue binding operational directives, which are compulsory orders for federal agencies to take action to safeguard information and IT systems when a security vulnerability has been identified.

Unfortunately, these authorities are generally viewed as reactive measures that open the Department up to costly liability and litigation and are not agile enough to address today's supply chain threats.

DHS needs the proper authorities to be able to decisively act when a threat to its supply chain has been identified. That is why, in the near term, I will be joining with my colleague Chairman King in introducing legislation to provide DHS with the tools to effectively carry out supply chain risk management in order to secure its supply chain.

Modeled after statutory authority given to the Department of Defense in 2011, this legislation will empower the Secretary of DHS to block entities who pose a security risk from being a DHS vendor. The legislation will also encourage information sharing across the Department when a supply chain risk has been identified.

I want to thank our distinguished panel for testifying this morning and I look forward to learning more about supply chain risk management at the Department. It is my intention to use today's discussion to help further shape a legislative solution for securing DHS's supply chain.
Thank you and I yield back the balance of my time.

###