Statement of Subcommittee Chairman Peter King (R-NY)
Joint Subcommittee Hearing

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

July 12, 2018

Remarks as Prepared

There is no question that nation states and criminal actors are constantly trying to exploit U.S. Government and private sector systems to steal information or insert potentially harmful hardware or software. The recent cases involving Kaspersky, ZTE and Huawei underscore the threats posed to the Federal supply chain and the urgency in developing stronger mechanisms to secure it.

In a March 2017, the Office of the Director of National Intelligence (ODNI) released a background paper on the supply chain risk management stating:

"Even as the U.S. government and private sector have implemented programs to mitigate and counter supply chain threats, the evolution of directed, sophisticated and multifaceted threats threatens to outpace our countermeasures. Traditional remedies such as trade agreements, economic sanctions, and legal actions are reactionary in nature and cannot keep pace with the evolution of threats."

The Federal Government is behind the curve in establishing robust supply chain security measures. It is clear that additional tools, policies, resources, and legal authorities are urgently needed to address this challenge.

I am pleased that the White House released a legislative proposal on Tuesday developed through the interagency process initiated in April. The proposal seeks to strengthen SCRM [pronounced: SCRIM] efforts across the government, enhance information sharing, and harden the Federal procurement process to identify and mitigate threats.

Additionally, I want to highlight that DHS is making great strides to implement SCRM measures throughout the Department. Last year, DHS issued policy directives for high value assets requiring that all DHS Components develop and implement SCRM strategies for sensitive systems, educate and train staff and contractors about supply chain risks, and enforce good supply chain hygiene by establishing contractual requirements and audit mechanisms for suppliers.

The purpose of today's hearing is to review current capabilities and authorities and assess whether additional authorities are needed to better protect the Department of Homeland Security's supply chain.

The Department of Defense and the Intelligence Community have existing authorities to block certain procurement efforts if security risks are identified. Even now, more is being done to protect their sensitive supply chain. The recently passed National Defense Authorization Act enhances DOD's authorities and the Intelligence Authorization Act, on the Floor today, further strengthens the Intelligence Communities SCRM toolkit. As a national security agency, it is vital that DHS also have robust supply chain risk management practices and tools to identify, mitigate and remove potential threats to its systems and contracts.

In addition to reviewing the OMB proposal, both Subcommittees are working on specific legislation to provide DHS with similar SCRM authorities to DOD. At the end of the day, the ability of any agency to address supply chain risk survives on a robust intelligence framework.

The foundation of any SCRM program is the ability to proactively identify entities seeking to exploit the DHS acquisition process, become trusted vendors, and then steal from or otherwise harm the homeland security enterprise.

In order to fully understand current DHS intelligence SCRM capabilities and specific threats to the supply chain, I expect that after an initial round of questions in the open session we will move into a closed session to better discuss those issues.

I again want to thank the witnesses for being here and express appreciation for Chairman Perry and Ranking Member Correa for working with us on this joint hearing.

###