Statement of Ranking Member J. Luis Correa (D-CA)

Subcommittee on Oversight and Management Efficiency Joint Hearing:

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

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

This morning the two subcommittees will hear from several distinguished witnesses on DHS's current authority related to mitigating threats to its supply chain. As previously mentioned by my colleagues in their opening statements, the U.S. needs a national strategy for supply chain risk management – and it needs it now.

Foreign nation-states like Russia and China rely on information and communication technology as a "strategic sector," in which the two countries' governments have invested significant capital and exercise substantial influence.

In 2012, the House Permanent Select Committee on Intelligence found that the risks posed by China's largest telecommunications manufacturers, ZTE and Huawei, "could undermine core U.S. national-security interests." In 2017, after "concern[s] about the ties between certain Kaspersky officials and Russian intelligence," DHS directed all Federal agencies to remove the Russian-based firm's products from their networks.

The exploitation of IT products and services through the global supply chain is a threat that continues to evolve each day. Bad actors continue to target U.S. government contractors and other private sector entities that do business with the government to try to gain advantage and pursue other state goals.

Over the past year, DHS has taken several steps to mitigate the risk and secure the Federal government's supply chain. Just recently, DHS launched a new Supply Chain Risk Management (SCRM), or "SKRIM" Program, within its National Programs and Protection Directorate. This new office was established to examine security concerns arising from the use of certain vendors and subcontractors.

However, while the goals of the Program are laudable, its mission far exceeds its resources. As of May, there were only two employees dedicated to the Program.

Considering that the risk is great, I hope to work with the Department and my colleagues across the aisle on providing this office with the proper resources and manpower that it deserves. Especially when we are considering expanding DHS's authority related to denying procurements based on national security concerns.

Lastly, I look forward to hearing from today's witnesses on how the DHS SCRM Program fits into the Federal government's overarching approach to supply chain security.

Without a Cybersecurity Coordinator within the Trump Administration, I am concerned about the White House's ability to consolidate the numerous efforts underway within multiple Federal agencies to address the national security implications of supply chain vulnerabilities.

The Federal government's supply chain is a target for our adversaries, and we need to ensure that commercial off the shelf goods and services are not subject to manipulation. Hence why it is imperative that we streamline these efforts to better protect against supply chain threats, and I hope to see the Administration work towards this.