Statement before the
Senate Committee on the Judiciary
"China's Non-Traditional Espionage Against the United States:
The Threat and Potential Policy Responses,"

A Testimony by:

James Mulvenon, Ph.D.
General Manager, Special Programs Division
SOS International, LLC

December 12, 2018

Dirksen Senate Office Building 226

Introduction and Main Points

Chairman Grassley, Ranking Member Feinstein, and distinguished members, thank you for inviting me to testify today.

While Chinese cyber threats and clandestine spying against the United States dominate the public discourse, a far more serious and insidious threat is posed by China's informal or 'extralegal' transfers of US technology. Operating under the radar, these quiet diversions of US technical know-how are carried out by groups and individuals in the US, whose support for China erodes America's technological edge and ability to compete in international markets. These groups on American soil, whose declared purpose is to "serve" (服务) a foreign power, are a fifth column of de facto agents managed by a professional cadre of Chinese government and government-associated S&T transfer specialists, who facilitate these property "exchanges" through a maze of venues, the particulars of which have only recently come to light.[i]

After years of appeasement and calls for patience under the pretense that China will acquiesce to international norms governing trade and the scientific endeavor, we must act to preserve what competitiveness we have left. Regardless of whether these informal transfers of US technology are legal (or illegal), the real danger lies in the fact that US regulators have no visibility into what leaves our country; whether it is owned by or merely accessible to these agents; and whether the technology is or should be under export restriction or protected to maintain our competitiveness. The mystery extends to the China end of the trans-Pacific pipeline as these US technologies and their human vectors disappear into an array of returnee parks, "national tech transfer centers," innovation incubators, and debriefing facilities into which US authorities also lack insight.

The following points, taken from peer-reviewed research in Chinese language open sources and corroborated by investigative journalists,[ii] illustrate the nature and dimensions of the problem:

- Chinese non-traditional espionage is not done randomly by overzealous individuals acting on their own. Rather, China has quietly enacted some two dozen laws creating a state-run foreign technology transfer apparatus that sponsors, for example, labs in China that are informed wholly by compatriots working abroad; databases of foreign co-optees; stipends, sinecures and cash to foreign donors of high-tech innovations; and the care and feeding of agents willing to "serve China while in place" abroad.

- Participants travel from the US at Chinese government expense, divulge technical knowledge through scripted venues, are briefed on China's technology interests, return to their US "base" (基地) for more information, and repeat the process. China has a program for what it euphemistically calls "short-term visits" by co-opted foreigners, which stripped of its rhetoric is indistinguishable from state-run espionage.

- Many Sino-US S&T "cooperation" organizations in the United States facilitate these transfers and have individual memberships of hundreds to thousands. The figure scales to some 90 such groups worldwide. Members usually are expatriate Chinese, although China is expanding its recruitment of non-ethnic Chinese.

- China S&T advocacy groups in the US declare loyalty to China and acknowledge a "duty" to support China's development through host country assets. Members visit China to lecture, guide Chinese technical projects, transfer technologies and help them take root, receive shopping lists from Chinese entities, and engage in other kinds of "technical exchanges." Many of them sit on Chinese government boards that decide the future of China's national technology investment.

- Chinese government tech transfer offices, facilitation companies, and career transfer personnel, some of whom are posted to China's diplomatic offices, support and direct the US-based groups. At the China end of it, hundreds of government offices are devoted entirely to facilitating foreign transfers of technology "by diverse means."

- China's unbridled effort to exploit foreign innovation is further seen in its open source acquisition infrastructure, which surpasses that of all other countries, probably combined. China employs a cadre of thousands to locate, study, and disseminate foreign journals, patents, proceedings, dissertations, and technical standards without regard to ownership or copyright restrictions. The documents are indexed, archived, and supplied to Chinese commercial and military "customers."

- According to NSA Director Keith Alexander, cyber espionage by Chinese state actors is massive, resulting in the "greatest transfer of wealth in human history." Cyber espionage is both a means for pilfering U.S. science and technology, as well as a method of intelligence collection for potential attacks against American military, government, and commercial technical systems. As a result, these cyber intrusions represent a fundamental threat to American economic competitiveness and national security.

- Ultimately foreign technology is converted in China into products and weapons at 180 "Pioneering Parks for Overseas Chinese Scholars," 160 "Innovation Service Centers," 276 "National Technology Model Transfer Organizations" and an unknown number of "technology business incubators." These large, ultra modern facilities are strategically located to insure wide distribution of the foreign technologies informally obtained.

Given the pace of technology development, its importance to a nation's economy and its national security, and the fact that a country's place in the world depends, today and tomorrow, on its scientific know-how, we need to fundamentally rethink our approach to protecting our future. US research, technology, processes and know-how are not a throw-away or sidebar in the bilateral relationship but a driver of future US competitiveness and should be protected as such. Responding to this threat requires a comprehensive effort across the three branches of government working in concert with the private sector, focused on specific executive orders, legislation and regulatory measures to repel Chinese efforts to subvert U.S. economic and national security.

[i] Hannas, Mulvenon, Puglisi, Chinese Industrial Espionage. Routledge, 2013.
[ii] (Cite Didi and Ed's four articles.)