Published on *The National Law Review* https://natlawreview.com

The Department of Justice's National Security Division Chief Addresses China's Campaign to Steal U.S. Intellectual Property

Article By:

David H. Laufman

Joseph M. Casino

Michael J. Kasdan

On August 12, 2020, John Demers, the head of the National Security Division (NSD) at the Department of Justice (DOJ), spoke publicly about national security threats from China at an event sponsored by the Center for Strategic and International Studies in Washington, DC. In more candid remarks than typically provided in a public forum, Mr. Demers concentrated on China's efforts to steal U.S. intellectual property (IP) from U.S. companies and other institutions, and how DOJ's "China Initiative" seeks to counter this threat.

Today's Altered Threat Environment

Mr. Demers reinforced that China is predominantly responsible for the theft of U.S. intellectual property, and that the insider threat is a growing problem:

- Over 80% of all cases charged as economic espionage (*i.e.*, cases involving the theft of trade secrets by or on behalf of the Chinese government or its instrumentalities or agents) involve China, and 60% of all trade secret cases involve China.

- China's typical *modus operandi* is to steal American IP, replicate it, replace the U.S. company originating that IP in the Chinese domestic market, then displace the United States in the global market.

- Recent years have seen increased involvement by China's intelligence service in the theft of IP: since 2014, responsibility for stealing American IP has shifted from cyber operations conducted by the People's Liberation Army (PLA) to insider-focused operations conducted by the Ministry of State Security (MSS), the intelligence and security agency for China

responsible for counter-intelligence, foreign intelligence and political security.

- The MSS, Mr. Demers observed, is good at developing relationships with individuals at U.S. companies who have access to IP, and many of DOJ's trade secret prosecutions now result from insider threats.

- China's "Thousand Talents" program serves as a vehicle for acquiring American IP. Individuals applying for the program, Mr. Demers stated, must demonstrate that they will bring IP to China. Some take U.S. IP to China and get paid for work performed in China; others simply hand over the IP to Chinese authorities.

- One hallmark of criminal cases charging individuals participating in the Thousand Talents program is that they conceal their affiliation with the program – either from the U.S. government, where a federal grant is involved, or from a university or other institution with which they are affiliated.

The scale of Chinese operations to steal American IP is also influencing the U.S. Government's strategy for countering this threat:

- DOJ has increased the number of prosecutors in NSD's Counterintelligence and Export Control Section (which has responsibility for prosecuting economic espionage) to work on China-related cases, and the FBI also has increased its dedicated resources.

- But the government has recognized that it "cannot prosecute our way" through the IP threat, Mr. Demers stated.

- Instead, where possible, the government now seeks to disrupt malign Chinese government activities.

- The Chinese consulate in Houston -- where PLA officials were based who had not disclosed their affiliation to the U.S. Government -- had "long been on the FBI's radar screen" for its involvement in IP theft in the United States, including its involvement in the Thousand Talents program. Its closure in July 2020 by the U.S. Government was part of the effort to disrupt Chinese operations.

- The government's disruption activities also includes increased, "targeted" screening of outbound Chinese students at U.S. airports, where they may be questioned about their fields of study and what institutions they are affiliated with in China.

Countering the Insider Threat

Given the shift in China's tactics, U.S. companies must be proactive in protecting their valuable intellectual property from insider threats, and they should think broadly in considering the potential universe of threats. Insiders include not only employees, but contractors, business partners, and possibly entities in their supply chain -- essentially, anyone with the authorized ability to access their internal systems and resources. Companies therefore should focus *less* on a given person's *job title*, for example, and concentrate *more* on the universe of people who have *access* to the information the company cares most about. Ultimately, the focus must be on identifying the "*malicious* insider" -- someone who not only has *authorized* access, but intentionally *exceeds* or *abuses* it for nefarious reasons.

Network monitoring, consistent with applicable federal and state laws, is certainly essential to detect suspicious insider behavior, as well as external intrusions. But purely technical tools are not enough to implement a robust insider threat mitigation program. Rather, *human* intelligence-gathering, judgment, and analysis -- focused on *human* behavior -- is essential, too.

The FBI has identified multiple behavioral indicators that an employee could be stealing a company's intellectual property, including:

- Without need or authorization, taking proprietary material home via documents, thumb drives, or other digital media;
- Manifesting interest in matters outside the scope of the employee's duties, particularly those of interest to foreign entities or business competitors;
- Working odd hours without authorization, and remotely accessing the computer network at odd times;
- Unexplained affluence;
- Unreported foreign contacts; and
- Short trips to foreign countries for unexplained or strange reasons.

Several corporate best practices have emerged to identify and respond to insider threats. As a threshold matter, companies should create and implement an insider threat program that has the support and resource commitment of the company's board of directors and executive management, as well as cross-organizational participation by components such as human resources, internal auditing, and legal counsel. Companies should make sure they have an incident response plan in which all company stakeholders participate – and make sure they rehearse it.

Correspondingly, companies should create a dedicated insider threat team to implement that program. In implementing an insider threat program, companies should:

- Develop an inventory of their most valuable intellectual property, who has authorized access

to it, and by what vectors.

- Develop criteria for anomalous behavior to focus the operations of the insider threat program.
- Develop and provide regular training and awareness programs for all personnel.
- Use technical tools, such as network monitoring software, identity and access management controls, and data loss prevention tools to monitor employee behavior on company networks. In this regard, companies should consider artificial intelligence applications to identify or warn of insider threat risks.

Technology solutions must be accompanied by intelligence-based human analysis to interpret technical data and bring judgment to the identification and evaluation of anomalous behavior. But whatever the mix of monitoring and analytical tools that companies employ to identify risk, they should ensure that these tools are employed in an objective, evidence-based manner.

National Law Review, Volume X, Number 237