CLIENT ALERT

DOJ Appointments at the Top and Recent Enforcement Actions Signal That Its China Initiative Will Likely Remain Intact

Apr.23.2021

Recent confirmations of the U.S. Department of Justice's ("DOJ's") senior leadership and enforcement actions coupled with the continued tough stance that the Biden administration is taking towards China signal that the DOJ's China Initiative will likely remain a strategic priority. Announced in 2018, the China Initiative, led by the DOJ's National Security Division, seeks to counter national security threats presented by the government of China by investigating and prosecuting economic espionage, trade secret theft, hacking, and other economic crimes. The China Initiative also focuses on protecting the nation's critical infrastructure against external threats through foreign direct investment and supply chain compromises, as well as combatting covert efforts to influence the American public and policymakers without proper transparency. According to DOJ, "[a]bout 80 percent of all economic espionage prosecutions brought by the U.S. Department of Justice (DOJ) allege conduct that would benefit the Chinese state, and there is at least some nexus to China in around 60 percent of all trade secret theft cases."

On Tuesday, April 20, 2021, a former head of DOJ's National Security Division, Lisa Monaco, was confirmed as the Deputy Attorney General, the No. 2 role at the Justice Department, by a near-unanimous vote of 98-2. As Deputy Attorney General, Monaco will manage the day-to-day activities of DOJ and serve as the main intermediary between Attorney General Merrick Garland and the individual components he leads, including the National Security Division. Monaco succeeds the Acting Deputy Attorney General, John Carlin, another former head of the National Security Division, who will become Monaco's top deputy. Tensions with China are likely to be top of mind for DOJ leadership, particularly in light of recent reports by a private cybersecurity firm working with the federal government that sophisticated Chinese government hackers are believed to have compromised dozens of U.S. government agencies, defense contractors, financial institutions, and other critical areas.

The day before Monaco's confirmation by the Senate, DOJ announced that Yu Zhou, a biotech researcher in a medical lab at Nationwide Children's Hospital Research Institute in Ohio ("Nationwide"), was sentenced to 33 months in prison for conspiring to steal trade secrets concerning the research, identification, and treatment of a range of pediatric medical conditions. Zhou and his wife, Li Chen, a fellow biotech researcher at the hospital, had earlier pleaded guilty to stealing trade secrets related to exosome isolation technology, which represents a critical development in the diagnosis and treatment of pediatric diseases, including liver cancer and a condition found in premature babies. For her role in the scheme, Chen was sentenced in February to 30 months in prison.

All of this activity follows on the heels of last week's testimony by Christopher Wray, the Director of the Federal Bureau of Investigation, that the Bureau has more than 2,000 investigations underway that lead back to the Chinese government, a 1,300% increase in recent years. "We're opening a new investigation into China every 10 hours, and I can assure you it's not because our folks don't have anything else to do with their time," Wray told the Senate Select Committee on Intelligence at its annual global threats hearing. Wray testified the day after DOJ revealed a FBI cyber operation to remove Chinese malware from U.S. servers.

Cyber-enabled theft of trade secrets, both by individual malicious actors and through State-sponsored intrusions, remains a profound challenge for government, industry, and research institutes. The wife-and-husband case of Chen and Zhou, however, illustrates a different threat vector for any organization with cutting edge technical research, including a children's research hospital, and a Chinese government hungry for valuable intellectual property. Specifically, according to the court filings, the long-time and trusted research scientists founded their own company in China in 2015, while still employed by Nationwide but without the hospital's knowledge, to market and sell products developed using Nationwide's proprietary technology. They also applied for patents in China to cover the exosome isolation technology, applied for research support from the Chinese National Natural Science Foundation, and allegedly received payments from China's State Administration of Foreign Expert Affairs. In 2017, the couple co-founded an American biotech company, GenExosome Technologies, which also marketed products and services related to this technology. The couple received more than $876,000 in cash and stocks related to an asset purchase agreement with the company and Zhou was set to make an additional $450,000 from a separate stock purchase agreement. As part of their convictions, the couple will forfeit approximately $1.45 million and were ordered to pay $2.6 million in restitution.

The indictment of Chen and Zhou represents the evolution of the cases brought under the DOJ's China Initiative to include a focus on non-traditional collectors of information, a term used to refer to researchers in labs, universities, and the defense industrial base that are being coopted into transferring technology contrary to U.S. interests. Perhaps most notably, these indictments have included those of a renowned Harvard professor as well as an MIT professor in connection with tax offenses, making false statements, and failing to disclose contracts, appointments, and rewards from various People's Republic of China ("PRC") entities to the U.S. government. Most recently, on April 22, 2021, a federal jury in Greeneville, Tennessee, convicted a U.S. citizen, Dr. Xiaorong You, of conspiracy to steal trade secrets, economic espionage, and wire fraud. According to court documents and evidence presented at trial, You stole valuable trade secrets as an employee of two U.S. companies related to formulations for bisphenol-A-free (BPA-free) coatings for the inside of beverage cans, while You and her Chinese corporate partner received millions of dollars in Chinese government grants to set up a new BPA-free coating company in China.

The guilty verdict follows a string of charges by DOJ as part of the China Initiative. On April 21, 2021, a federal grand jury in Carbondale, Illinois returned an indictment charging a mathematics professor and researcher at Southern Illinois University – Carbondale (SIUC) with two counts of wire fraud and one count of making a false statement. According to court documents, Mingqing Xiao fraudulently obtained $151,099 in federal grant money from the National Science Foundation by concealing support he was receiving from the Chinese government and a Chinese university. In February, DOJ indicted a Chinese businessman for allegedly conspiring to steal proprietary data from General Electric ("GE") and produce and sell it in China. That same month, a federal grand jury issued a superseding indictment charging a researcher at Stanford University with visa fraud, obstruction of justice, destruction of documents, and false statements in connection with an alleged scheme to conceal and lie about her status as a member of the PRC's military forces while in the United States. A few weeks earlier, a former University of Florida (UF) professor, researcher, and resident of China was indicted for fraudulently obtaining $1.75 million in federal grant money from the National Institutes of Health (NIH). The former UF professor is accused of concealing support he received from the Chinese government and a company that he founded in China to profit from that research.

The continuation of the line of cases focused on holding those who attempt to steal or unlawfully acquire proprietary trade secrets, research, and intellectual property accountable illustrates that the U.S. government remains vigilant against attacks by those seeking to pilfer our nation's greatest assets: our knowledge, technology, and innovations. Protecting against these vulnerabilities will continue to be a tall order – and should be a top priority – for government, industry, and research institutes.

Crowell & Moring regularly advises clients on ways to protect against the theft of their trade secrets from both external and internal threats. Getting sound legal advice early in the process helps to identify and secure these critical assets, address external breaches or internal misappropriations that occur, preserve evidence and affirmative relief, and respond to allegations by competitors.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Michael K. Atkinson
Partner – Washington, D.C.
Phone: 202.624.2540
Email: matkinson@crowell.com

Caroline E. Brown
Partner – Washington, D.C.
Phone: +1 202.624.2509
Email: cbrown@crowell.com

Julia Milewski
Partner – Washington, D.C.
Phone: +1 202.624.2514
Email: jmilewski@crowell.com

Laura Schwartz
Counsel – Los Angeles
Phone: +1 213.443.5581
Email: lschwartz@crowell.com