September 2018

Monthly Counterintelligence Bulletin

New FBI Resources Educate Public about Threats Posed by Malign Foreign Influence Operations

The FBI launched a suite of resources on August 30 to educate the public about the threats posed by disinformation campaigns and cyberattacks, as well as the overall impact of malign foreign influence on society. In its role as the lead federal agency responsible for investigating malign foreign influence operations, the FBI has launched the Protected Voices initiative to mitigate the risk of cyber influence operations targeting U.S. elections and raise awareness among political campaigns about the best ways to fend off attempts to infiltrate their information technology infrastructure. Visit the FBI's malign foreign influence website.

National Institutes of Health Issues Statement on Protecting Integrity of U.S. Biomedical Research

National Institutes of Health Director Francis S. Collins released a statement on August 23 emphasizing the importance of protecting the integrity of U.S. biomedical research from foreign influence. The statement cited growing concerns regarding the diversion of intellectual property to other countries, peer reviewers who have shared confidential information with foreign entities, and the failure of NIH-funded institutions to report substantial contributions from foreign governments. In response, Director Collins announced NIH will collaborate with U.S. government agencies, professional organizations, and the academic institutions it funds to more effectively mitigate the risk to intellectual property, safeguard the integrity of peer review, and improve reporting on affiliations, financial interests, and sources of research support. Read the statement.

Two Scientists Plead Guilty to Stealing Trade Secrets to Benefit Chinese Pharmaceutical Company

Two scientists recently pleaded guilty to their roles in a conspiracy to steal trade secrets from GlaxoSmithKline to benefit a China-based pharmaceutical company. Pennsylvania resident Yu Xue was working as a scientist for GSK when she, California resident Tao Li, and another conspirator, Yan Mei, received financial support and subsidies from the Chinese government to form Renopharma in Nanjing, China, to research and develop anti-cancer drugs. Xue then sent a large quantity of GSK scientific documents—some of which included confidential information and trade secrets regarding research data, biopharmaceutical processes, and products in development—to Li and Mei at Renopharma. Xue pleaded guilty on August 31 and is scheduled to be sentenced in December; Li pleaded guilty on September 14 and is scheduled to be sentenced in

January 2019. Both face a maximum of 10 years in prison, as well as potential fines and forfeiture of assets. Read about the pleas.

Four Chinese State-Owned Industrial Companies Arraigned in Economic Espionage Conspiracy

Four Chinese state-owned companies were arraigned on September 6 on a third superseding indictment charging them and two of their officers with conspiracy to commit economic espionage and attempted economic espionage. According to the indictment, between 1998 and 2011, Pangang Group Co. conspired with Hou Shengdong and Dong Yingjie, as well as three of the company's subsidiaries and others, to acquire stolen or misappropriated trade secrets from DuPont regarding the production technology for chloride-route titanium dioxide. If convicted, the companies face a maximum sentence of five years of probation and a $10 million fine for each count, and Hou and Dong face up to 15 years in prison, three years of supervised release, and a $500,000 fine for each count. The indictment also seeks the potential forfeiture of assets. Read about the charges.

Media Highlight

The following information has been prepared by outlets outside the U.S. government and has not been corroborated by the FBI or its partners. It is presented here for your situational awareness.

***TechCrunch* Report Details Defense Bill's Prohibition of Five Chinese Firms' Technology**

An article published on August 14 by online technology publication *TechCrunch* highlighted language in the National Defense Authorization Act for fiscal year 2019 prohibiting U.S. government agencies from using or procuring technology produced by several Chinese firms. Citing national security concerns, the legislation—which was signed into law in August and will go into effect over the next two years—specifically forbids government agencies and contractors from using telecommunications and video surveillance hardware produced by Huawei, ZTE, Hytera, Hikvision, and Dahua, according to the report. Read the *TechCrunch* article.

This Monthly Counterintelligence Bulletin is prepared by the FBI's Counterintelligence Division.
To report a counterintelligence matter, contact your local FBI office.