Session ###: What the DOJ’s “China Initiative” Means for White Collar Prosecutions

On November 1, 2018, the U.S. Department of Justice announced the creation of a “China Initiative,” focused on a host of potential regulatory and criminal violations involving China, such as the theft of trade secrets, violations of the Foreign Agents Registration Act, and violations of the Foreign Corrupt Practices Act. Was that announcement merely saber rattling by the U.S. government or has it had tangible effects?

Come hear from veteran practitioners from leading global law firms and the U.S. Department of Justice discuss the ramifications of the China Initiative on companies and individuals doing business in China and/or with Chinese companies and individuals. Discussion topics will include: (1) recent high-profile cases involving Chinese companies and individuals, including the prosecution of Huawei and Meng Wanzhou; (2) what the DOJ’s recent focus means for attorneys representing companies and individuals with any connection to China; and (3) an overview of major compliance and enforcement risks for companies and individuals doing business with China.

**Moderator:**
Edward Y. Kim, Krieger Kim & Lewin LLP

**Speakers:**
John P. Cronan, Principal Deputy Assistant Attorney General, U.S. Department of Justice
Joon H. Kim, Cleary Gottlieb Steen & Hamilton LLP
Tai H. Park, White & Case LLP
Jeannie S. Rhee, Paul, Weiss, Rifkind, Wharton & Garrison LLP
Basics of the DOJ’s “China Initiative”

- Announced by former Attorney General Jeff Sessions on November 1, 2018
  - “But under President Donald Trump, the United States is standing up to the deliberate, systematic, and calculated threats posed, in particular, by the communist regime in China, which is notorious around the world for intellectual property theft.”
  - “We are here today to say: enough is enough. We’re not going to take it anymore. It is unacceptable. It is time for China to join the community of lawful nations. International trade has been good for China, but the cheating must stop. And we must have more law enforcement cooperation; China cannot be a safe haven for criminals who run to China when they are in trouble, never to be extradited. China must accept the repatriation of Chinese citizens who break U.S. immigration law and are awaiting return.”

- Stated goals of the China Initiative:
  - Identify priority trade secret theft cases, ensure that investigations are adequately resourced, and work to bring them to fruition in a timely manner and according to the facts and applicable law;
  - Develop an enforcement strategy concerning non-traditional collectors (e.g. researchers in labs, universities, and the defense industrial base) that are being coopted into transferring technology contrary to U.S. interests;
  - Educate colleges and universities about potential threats to academic freedom and open discourse from influence efforts on campus;
  - Apply the Foreign Agents Registration Act (FARA) to unregistered agents seeking to advance China’s political agenda, bringing enforcement actions when appropriate;
  - Equip the nation’s U.S. Attorneys with intelligence and materials they can use to raise awareness of these threats within their Districts and support their outreach efforts;
- Implement the Foreign Investment Risk Review Modernization Act (FIRMA) for DOJ;

- Identify opportunities to better address supply chain threats, especially ones impacting the telecommunications sector, prior the transition to 5G networks;

- Identify Foreign Corrupt Practices Act (FCPA) cases involving Chinese companies that compete with American businesses;

- Increase efforts to improve Chinese responses to requests under the Mutual Legal Assistance Agreement (MLAA) with the United States; and

- Evaluate whether additional legislative and administrative authorities are required to protect our national assets from foreign economic aggression.

- Types of offenses that might be more frequently charged as a result of the China Initiative:
  
  - **Foreign Corrupt Practices Act (FCPA) (15 U.S.C. §§ 78dd-1, et seq.)**

    - “a) **Prohibition** It shall be unlawful for any issuer which has a class of securities registered pursuant to section 78l of this title or which is required to file reports under section 78o(d) of this title, or for any officer, director, employee, or agent of such issuer or any stockholder thereof acting on behalf of such issuer, to make use of the mails or any means or instrumentality of interstate commerce corruptly in furtherance of an offer, payment, promise to pay, or authorization of the payment of any money, or offer, gift, promise to give, or authorization of the giving of anything of value to—(1) any foreign official for purposes of— (A)(i) influencing any act or decision of such foreign official in his official capacity, (ii) inducing such foreign official to do or omit to do any act in violation of the lawful duty of such official, or (iii) securing any improper advantage; or (B) inducing such foreign official to do his influence with a foreign government or instrumentality thereof to affect or influence any act or decision of such government or instrumentality, in order to assist such issuer in obtaining or retaining business or with, or directing business to, any person; (2) any foreign political party or official thereof or any candidate for foreign political office for purposes of— (A) (i) influencing any act or decision of such party, official, or candidate in its or his official capacity, (ii) inducing such party, official, or candidate to do or omit to do an act in violation of the lawful duty of such party, official, or candidate, or (iii) securing any improper advantage; or (B) inducing such party, official, or candidate to do or omit to do an act in violation of the lawful duty of such party, official, or candidate, or
official, or candidate to use its or his influence with a foreign government or instrumentality thereof to affect or influence any act or decision of such government or instrumentality, in order to assist such issuer in obtaining or retaining business for or with, or directing business to, any person; or (3) any person, while knowing that all or a portion of such money or thing of value will be offered, given, or promised, directly or indirectly, to any foreign official, to any foreign political party or official thereof, or to any candidate for foreign political office, for purposes of-- (A)(i) influencing any act or decision of such foreign official, political party, party official, or candidate in his or its official capacity, (ii) inducing such foreign official, political party, party official, or candidate to do or omit to do any act in violation of the lawful duty of such foreign official, political party, party official, or candidate, or (iii) securing any improper advantage; or (B) inducing such foreign official, political party, party official, or candidate to use his or its influence with a foreign government or instrumentality thereof to affect or influence any act or decision of such government or instrumentality, in order to assist such issuer in obtaining or retaining business for or with, or directing business to, any person.”

- **Elements:**

  - Under either of the accounting provisions, the defendant must “knowingly circumvent or knowingly fail to implement a system of internal accounting controls or knowingly falsify any book, record or account.” Although the intent requirement is designed to reduce potential liability for inadvertent accounting violations, the “knowing” requirement is met by willful blindness.

  - “(i) a U.S. “issuer,” “domestic concern,” or “any person,” including the officers, directors, employees, agents, or shareholders acting on behalf of the issuer, domestic concern, or person, (ii) makes use of the mails or any means or instrumentality of interstate commerce, (iii) in furtherance of an offer, payment, promise to pay, or authorization to pay anything of value, (iv) to any foreign official, any foreign political party or official thereof, or any candidate for foreign political office, or other person, knowing that the payment to that other person would be passed on to a foreign official, foreign political party or official thereof or candidate for foreign political office, (v) inside the territory of the United States or, for any United States personality, outside the United States, (vi) to corruptly (vii) influence any official act or decision, induce an action or an omission to act in violation of a lawful duty, or to secure any improper advantage, (viii) or induce
any act or decision that would assist the company in obtaining, retaining, or directing business to any person.”1

- **Foreign Agents Registration Act (FARA) (22 U.S.C. § 611, et seq)**

  - 22 U.S.C. § 612 (a): “No person shall act as an agent of a foreign principal unless he has filed with the Attorney General a true and complete registration statement and supplements thereto as required by subsections (a) and (b) of this section or unless he is exempt from registration under the provisions of this subchapter. Except as hereinafter provided, every person who becomes an agent of a foreign principal shall, within ten days thereafter, file with the Attorney General, in duplicate, a registration statement, under oath on a form prescribed by the Attorney General. The obligation of an agent of a foreign principal to file a registration statement shall, after the tenth day of his becoming such agent, continue from day to day, and termination of such status shall not relieve such agent from his obligation to file a registration statement for the period during which he was an agent of a foreign principal…”

  - **Elements:**

    - The defendant acted as an agent, employee, or in any other capacity at the order, request, or under the direction or control of a “foreign principal,” or otherwise agreed, consented, or held himself out as an agent of a foreign principal; and

    - The defendant (i) engages within the United States in political activities for or in the interests of such foreign principal; (ii) acts within the United States as a public relations counsel, publicity agent, information-service employee or political consultant for or in the interests of such foreign principal; (iii) within the United States solicits, collects, disburses, or dispenses contributions, loans, money, or other things of value for or in the interest of such foreign principal; or (iv) within the United States represents the interests of such foreign principal before any agency or official of the Government of the United States

    - The defendant willfully failed to file a true and complete FARA registration within 10 days of becoming an agent of a foreign principal or violated any other requirement of the act (e.g., reporting, labeling, or document retention)

• No exemption applies.  

**Theft of Trade Secrets (18 U.S.C. § 1832)**

- “(a) Whoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly—(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information; (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information; (3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization; (4) attempts to commit any offense described in paragraphs (1) through (3); or (5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.”

**Elements:**

- “With respect to the substantive offense of theft of trade secrets, the Government must prove: (1) that the defendant intended to convert proprietary information to the economic benefit of anyone other than the owner; (2) that the proprietary information was a trade secret; (3) that the defendant knowingly stole, copied, or received trade secret information; (4) that the defendant intended or knew the offense would injure the owner of the trade secret; and (5) that the trade secret was included in a product that is placed in interstate commerce.”

• Recent, notable cases

  - **U.S. v. Huawei Technologies Co., Ltd., et.al. (EDNY) (Jan. 2019)**

---


- **Allegations:** The government has alleged that Huawei misrepresented to the U.S. government and several financial institutions that, although the company conducted business in Iran, it did not violate OFAC’s Iranian Transactions and Sanctions Regulations.

- **Status:** Pending/Discovery Ongoing; next status conference set for September 4, 2019


  - **Charges:** Conspiracy to Commit Theft of Trade Secrets and Attempted Theft of Trade Secrets, (18 U.S.C. § 1832), Wire Fraud (18 U.S.C. § 1343), and Obstruction of Justice (18 U.S.C. § 1512)

  - **Allegations:** The government has alleged that Huawei stole and attempted to steal trade secrets from T-Mobile, and then obstructed justice when T-Mobile threatened to sue Huawei.

  - **Status:** Pending; oral argument on Defendants’ Motion to Dismiss set for October 7, 2019


  - **Charge:** theft of trade secrets, 18 U.S.C. § 1832

  - **Allegations:** Zhang was charged with theft of trade secrets for allegedly stealing proprietary information from his employer, KCG. KCG, which has since been acquired by Virtu Financial, engaged in market making, high-frequency trading, electronic execution, and institutional sales and trading. According to the Complaint, Zhang installed code designed to
steal KCG’s computer code concerning algorithmic trading models and trading platforms, and accessed colleagues’ computer systems remotely without authorization.

- **Status:** Adjourned sine dia

- **U.S. v. Xiaoqing Zheng** (NDNY) (Aug 2018)
  - **Charge:** Theft of trade secrets, 18 U.S.C. § 1832
  - **Allegations:** Zheng was an engineer at General Electric’s Power Division in Schenectady, New York. According to the Complaint, Zheng downloaded over 19,000 files to his personal devices from GE, including confidential and proprietary information related to GE’s turbine technology. Zheng employed sophisticated methods, including encryption and steganography, to conceal his theft, which, according to the Complaint “are uncommon even among trained computer experts… and both GE digital analysts and FBI agents specializing in cyber crimes [stated] that they were aware of these measures in theory but had never actually seen a subject employ them.”
  - **Status:** Trial set for October 28, 2019

- **U.S. v. Xiaolang Zhang** (NDCA) (July 2018)
  - **Charges:** Theft of trade secrets, 18 U.S.C. § 1832
  - **Allegations:** Zhang was a hardware engineer at Apple’s autonomous vehicle development team. According to the Complaint, in April 2018, Zhang informed his supervisor at Apple that he would be resigning from the company to work at X-Motors, a Chinese company focused on autonomous vehicle technology. Shortly after, Apple’s New Product Security team reviewed Zhang’s user activity and learned that two days before his resignation, Zhang’s computer usage had increased exponentially, and he bulk searched and downloaded numerous proprietary and confidential files related to Apple’s autonomous vehicle development.
  - **Status:** Pending/discovery ongoing; next status conference set for September 23, 2019

- **U.S. v. Jiaqiang Xu** (SDNY) (Dec. 2015)
**Charges:** Theft of trade secrets, 18 U.S.C. § 1832, Economic Espionage

**Allegations:** Xu worked as a software engineer for a branch of IBM located in China. According to the Complaint, Xu provided IBM’s proprietary source code to undercover law enforcement officers posing as financial investors in an effort to gain employment with their start-up venture. In a Superseding Indictment, Xu was also indicted for three counts of economic espionage, one count theft of trade secrets, one count of distribution of trade secrets, and one count of possession of trade secrets. The Superseding Indictment alleges that Xu stole and converted IBM’s source code with the intent to benefit the People Republic of China’s National Health and Family Planning Commission.

**Status:** Plead Guilty; Sentenced to 60 months imprisonment

- *U.S. v. Shan Shi*, 17 Cr. 110 (DC) (June 2017)


**Allegations:** Shi and six others were indicted in June 2017 and charged with conspiring to steal trade secrets from Trelleborg Offshore, a Houston-based U.S. subsidiary of the Swedish engineering giant Trelleborg. The government alleged that Shan Shi, conspired to steal, possess and use trade secrets belonging to Trelleborg, which manufactured syntactic foam, for use in the oil drilling industry for the benefit of a foreign government, the People’s Republic of China. Shi was arrested at a meeting with undercover FBI agents posing as buyers with a U.S. defense contractor seeking to build undersea remote-operated vehicles. Of six co-defendants in the case, four pleaded guilty to conspiring to commit theft of trade secrets, and two who have been sentenced have received probation.

**Status:** Following a nine-day trial, Shi was convicted on one count of conspiracy to commit theft of trade secrets. He was acquitted on the other charges (money laundering, economic espionage).

- Examples of tools that the USG can use in extraterritorial investigations
  - MLAA/MLAT requests
Extradition / Provisional Arrest Warrants

International extradition is the formal process by which a person found in one country is surrendered to another country for trial or punishment. The process is regulated by treaty and conducted between the Federal Government of the United States and the government of a foreign country. It differs considerably from interstate rendition, commonly referred to as interstate extradition, mandated by the Constitution, Art. 4, Sec. 2.

Generally under U.S. law (18 U.S.C. § 3184), extradition may be granted only pursuant to a treaty. However, some countries grant extradition without a treaty, and of those that do, most require an offer of reciprocity. Further, 18 U.S.C. §§ 3181 and 3184 permit the United States to extradite, without regard to the existence of a treaty, persons (other than citizens, nationals or permanent residents of the United States), who have committed crimes of violence against nationals of the United States in foreign countries. A list of countries with which the United States has an extradition treaty relationship can be found in the Federal Criminal Code and Rules, following 18 U.S.C. § 3181, but consult the Criminal Division’s Office of International Affairs (OIA) to verify the accuracy of the information.

If the fugitive is not subject to extradition, other steps may be available to return him or her to the United States or to restrict his or her ability to live and travel overseas. See JM 9-15.600 et seq.

If a fugitive is apprehended only after a long delay, a prosecutor may have to litigate a motion alleging a constitutional speedy trial violation if extradition has not been sought or the Government has not been actively pursuing other steps to return the fugitive to the United States. All decisions to pursue or not to pursue extradition
or other measures to obtain custody of the fugitive should be documented to prepare for any eventual speedy trial motion.

- **JM 9-15.230 – Request for Provisional Arrest**

  - Every extradition treaty to which the United States is a party requires a formal request for extradition, supported by appropriate documents. Because the time involved in preparing a formal request can be lengthy, most treaties allow for the provisional arrest of fugitives in urgent cases. Once the United States requests provisional arrest pursuant to the treaty, the fugitive may be arrested and detained (or, in some countries, released on bail) following the issuance of an order of arrest by the foreign authorities. Thereafter, the United States must submit a formal request for extradition, supported by all necessary documents, duly certified, authenticated and, if necessary, translated into the language of the country where the fugitive was arrested, within a specified time (from 30 days to three months, depending on the treaty). See JM 9-15.240. Failure to follow through on an extradition request by submitting the requisite documents after a provisional arrest has been made will result in release of the fugitive, strains on diplomatic relations, and possible liability for the prosecutor.

  - OIA determines whether the facts of the case meet the requirement of urgency under the terms of the applicable treaty. If they do, OIA requests provisional arrest; if not, the prosecutor assembles the documents for a formal request for extradition. The latter method is favored when the defendant is unlikely to flee because the time pressures generated by a request for provisional arrest may result in errors that can damage the case. If provisional arrest is necessary because of the risk of flight, the prosecutor should complete the form for requesting provisional arrest and forward it, along with a copy of the charging document and arrest warrant, to OIA by email.

- **Alternatives to Extradition**

  - **JM 9-15.610 – Deportations, Expulsions, or Other Lawful Methods of Return**

    - If the fugitive is not a national or lawful resident of the country in which he or she is located, the OIA, through the Department of
State or other channels, may ask that country to deport, expel, or otherwise effectuate the lawful return of the fugitive to the United States.

- JM 9-15.630 – Lures

A lure involves using a subterfuge to entice a criminal defendant to leave a foreign country so that he or she can be arrested in the United States, in international waters or airspace, or in a third country for subsequent extradition, expulsion, or deportation to the United States. Lures can be complicated schemes or they can be as simple as inviting a fugitive by telephone to a party in the United States.

Some countries will not extradite a person to the United States if the person’s presence in that country was obtained through the use of a lure or other ruse. In addition, some countries may view a lure of a person from its territory as an infringement on its sovereignty or criminal law. Consequently, a prosecutor must consult with the OIA and secure approval from the Criminal Division before undertaking a lure. Prosecutors contemplating a lure should consult with OIA as early as possible. If OIA concurs with the lure proposal, OIA will recommend that a Deputy Assistant Attorney General (DAAG) in the Criminal Division approve the lure. Lure approval authority resides with the DAAG.

- JM 9-15.635 – Interpol Red Notices

An Interpol Red Notice is an international “lookout” and is the closest instrument to an international arrest warrant in use today. Please be aware that if a fugitive is arrested pursuant to a Red Notice, the prosecutor’s office is obligated to do whatever work is required to produce the necessary extradition documents within the time limits prescribed by the controlling extradition treaty or, in the absence of a treaty, the arresting country’s domestic law, whenever and wherever the fugitive is arrested. Further, the prosecutor’s office is obliged to pay the expenses pursuant to the controlling treaty.

Interpol Red Notices are useful when the fugitive’s location or countries to which he or she may travel, are unknown. Red Notices may be broadly distributed or tailored specifically to countries to which it is believed the fugitive will travel. For additional
information about Interpol Red Notices, see www.interpol.int//INTERPOL-expertise/Notices.

- Because many countries will arrest a fugitive based solely on a Red Notice, it is the responsibility of the prosecutor to inform Interpol if a Red Notice should be withdrawn.


  - The Department of State may revoke the passport of a U.S. citizen who is the subject of an outstanding Federal or State warrant. Revocation of a U.S. passport can result in loss of the fugitive’s lawful residence status in a foreign country, which may lead to his or her deportation

- JM 9-15.650 – Foreign Prosecution

  - If the fugitive has taken refuge in the country of which he or she is a national, and is thereby not extraditable, it may be possible to ask that country to prosecute the individual for the crime that was committed in the United States. This can be an expensive and time consuming process and in some countries domestic prosecution is limited to certain specified offenses. In addition, a request for domestic prosecution in a particular case may conflict with U.S. law enforcement efforts to change the “non-extradition of nationals” law or policy in the foreign country. Whether this option is available or appropriate should be discussed with OIA.

- JM 9-13.525 – Subpoenas

  - U.S. law, in the form of mutual legal assistance treaties, requires that the United States attempt to obtain records using the mutual legal assistance process prior to resorting to unilateral compulsory measures. Therefore, all Federal prosecutors must obtain written approval from the OIA before issuing any unilateral compulsory measure to persons or entities in the United States for records located abroad.

  - OIA must also be consulted prior to initiating enforcement proceedings relating to such processes. This includes situations where the prosecutor was unaware that the requested records were located abroad but is subsequently notified of that fact.
There are two clarifications to the above. First, some entities have taken the position that they will voluntarily provide records even when those records may be located abroad. In such cases, no prior consultation with OIA is required.

Second, prosecutors are not required to consult with OIA prior to seeking a search warrant pursuant to the Stored Communications Act to obtain records from a U.S.-based communications service provider, regardless of where those records may actually be located. See 18 U.S.C. § 2713. Prosecutors are strongly encouraged to consult with the Criminal Division’s Computer Crime and Intellectual Property Section if a service provider claims that the records called for by the warrant are not subject to U.S. jurisdiction.

The service of process in a foreign country of U.S. permanent residents and nationals pursuant to 28 U.S.C. § 1783 can also implicate sovereignty issues and, when done unilaterally, can adversely affect law enforcement relationships. MLATs and other forms of legal assistance mechanisms address requests for service of process abroad. You should consult with OIA prior to issuing a 28 U.S.C. § 1783 subpoena.

OIA approval must also be obtained prior to serving a subpoena ad testificandum on an officer of, or attorney for, a foreign bank or corporation who is temporarily in or passing through the United States when the testimony sought relates to the officer’s or attorney’s duties in connection with the operation of the bank or corporation.

The amended Rule 41(b)(6) does not authorize courts to issue warrants for the search of electronic information stored abroad. When conducted without consultation with foreign authorities, such searches may raise concerns, including adverse impacts upon the law enforcement and other relationships of the United States with foreign countries. The use of such searches can implicate foreign sovereignty and criminal law issues and may even lead to the filing of foreign criminal charges against the U.S. prosecutor or law enforcement agent involved in the search. Before applying for a warrant under either subsection of Rule 41(b)(6), reasonable efforts shall be used to identify whether the computer to be searched is located inside or outside the United States. Where the location of the computer is uncertain, but possibly within the United States, judicial approval will assure that Constitutional requirements have been met. Any warrant should be limited to authorizing a search only in the United States. To the extent the location of the computer cannot be definitively determined to be in a judicial district of the United States, but it is
reasonably possible that the location is in the United States, prosecutors should consider whether to limit their initial search to one which solely assists in the identification of the location of the computer. If there is reason to believe that the computer is in a specific foreign country, prosecutors should consult with the Office of International Affairs about appropriate coordination with foreign law enforcement partners as well as potential diplomatic and sovereignty issues before performing a remote search.

- JM 9-13.526 – Forfeiture of Assets Located in Foreign Countries

  - Both international and domestic coordination are needed in matters relating to the forfeiture of assets located in foreign countries. Consequently, any attorney for the Federal government who plans to file a civil forfeiture action for assets located in another country pursuant to 28 U.S.C. § 1355(b)(2) is directed to notify the Office of International Affairs (OIA) of the Criminal Division before taking such action.

  - Attorneys for the Federal government are also directed to coordinate with OIA in order to present to a foreign government, for enforcement or recognition, any civil or criminal forfeiture order entered in the United States for property located within the foreign jurisdiction.

  - In cases where it appears that the property in question is likely to be removed, destroyed, or dissipated so as to defeat the possibility of the forfeiture under U.S. law, the attorney for the Federal government may request OIA to seek the assistance of the authorities of the foreign government where the property is located to seize, restrain, or take other action necessary and appropriate to preserve the property for forfeiture.

- JM 9-13.525 — Search warrants

  - Prosecutors are not required to consult with OIA prior to seeking a search warrant pursuant to the Stored Communications Act to obtain records from a U.S.-based communications service provider, regardless of where those records may actually be located. See 18 U.S.C. § 2713. Prosecutors are strongly encouraged to consult with the Criminal Division’s Computer Crime and Intellectual Property Section if a service provider claims that the records called for by the warrant are not subject to U.S. jurisdiction.

- Office of Foreign Assets Control (OFAC) – Specially Designated Nationals (SDNs)
U.S. Department of the Treasury: “As part of its enforcement efforts, OFAC publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific. Collectively, such individuals and companies are called ‘Specially Designated Nationals’ or ‘SDNs.’ Their assets are blocked and U.S. persons are generally prohibited from dealing with them.”
ATTORNEY GENERAL JEFF SESSION’S CHINA INITIATIVE FACT SHEET

Background

The Attorney General’s Initiative reflects the Department’s strategic priority of countering Chinese national security threats and reinforces the President’s overall national security strategy. The Initiative is launched against the background of previous findings by the Administration concerning China’s practices. In March 2018, the Office of the U.S. Trade Representative announced the results of a months’ long investigation of China’s trade practices under Section 301 of the Trade Act of 1974. It concluded, among other things, that a combination of China’s practices are unreasonable, including its outbound investment policies and sponsorship of unauthorized computer intrusions, and that “[a] range of tools may be appropriate to address these serious matters.”

In June 2018, the White House Office of Trade and Manufacturing Policy issued a report on “How China’s Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World,” documenting “the two major strategies and various acts, policies, and practices Chinese industrial policy uses in seeking to acquire the intellectual property and technologies of the world and to capture the emerging high-technology industries that will drive future economic growth.”

The National Security Division (NSD) is responsible for countering nation state threats to the country’s critical infrastructure and private sector. In addition to identifying and prosecuting those engaged in trade secret theft, hacking and economic espionage, the initiative will increase efforts to protect our critical infrastructure against external threats including foreign direct investment, supply chain threats and the foreign agents seeking to influence the American public and policymakers without proper registration.

Statements

Attorney General Jeff Sessions

Chinese economic espionage against the United States has been increasing—and it has been increasing rapidly. Enough is enough. We’re not going to take it anymore. I have ordered the creation of a China Initiative led by Assistant Attorney General John Demers and composed of a senior FBI Executive, five United States Attorneys including Alex, and several other Department of Justice leaders and officials, including Assistant Attorney General Benczkowski. This Initiative will identify priority Chinese trade theft cases, ensure that we have enough resources dedicated to them, and make sure that we bring them to an appropriate conclusion quickly and effectively.

Assistant Attorney for National Security John C. Demers

“China wants the fruits of America’s brainpower to harvest the seeds of its planned economic dominance. Preventing this from happening will take all of us, here at the Justice Department,
Assistant Attorney General Brian Benczkowski

"To counter the threat of Chinese malign economic aggression, prosecutors in the Criminal Division are redoubling our efforts to aggressively investigate Chinese companies and individuals for theft of trade secrets," said Assistant Attorney General Brian Benczkowski. “We will work hard to do our part, in partnership with other Department components, to assure fairness in the global economic system.”

FBI Director Christopher Wray

"No country presents a broader, more severe threat to our ideas, our innovation, and our economic security than China," said FBI Director Christopher Wray. "The Chinese government is determined to acquire American technology, and they’re willing use a variety of means to do that – from foreign investments, corporate acquisitions, and cyber intrusions to obtaining the services of current or former company employees to get inside information.  If China acquires an American company's most important technology – the very technology that makes it the leader in a field – that company will suffer severe losses, and our national security could even be impacted.  We are committed to continuing to work closely with our federal, state, local, and private sector partners to counter this threat from China."

US Attorneys in Working Group

- Andrew E. Lelling (District of Massachusetts)
- Jay E. Town (Northern District of Alabama)
- Alex G. Tse (Northern District of California)
- Richard P. Donoghue (Eastern District of New York)
- Erin Nealy Cox (Northern District of Texas)

Components of Initiative

The Attorney General has set the following goals for the Initiative:

— Identify priority trade secret theft cases, ensure that investigations are adequately resourced; and work to bring them to fruition in a timely manner and according to the facts and applicable law;

— Develop an enforcement strategy concerning non-traditional collectors (e.g., researchers in labs, universities, and the defense industrial base) that are being coopted into transferring technology contrary to U.S. interests;

— Educate colleges and universities about potential threats to academic freedom and open discourse from influence efforts on campus;

— Apply the Foreign Agents Registration Act to unregistered agents seeking to advance China’s political agenda, bringing enforcement actions when appropriate;

— Equip the nation’s U.S. Attorneys with intelligence and materials they can use to raise awareness of these threats within their Districts and support their outreach efforts;

— Implement the Foreign Investment Risk Review Modernization Act (FIRMA) for DOJ (including by working with Treasury to develop regulations under the statute and prepare for increased workflow);

— Identify opportunities to better address supply chain threats, especially ones impacting the telecommunications sector, prior to the transition to 5G networks;
— Identify Foreign Corrupt Practices Act (FCPA) cases involving Chinese companies that compete with American businesses;
— Increase efforts to improve Chinese responses to requests under the Mutual Legal Assistance Agreement (MLAA) with the United States; and
— Evaluate whether additional legislative and administrative authorities are required to protect our national assets from foreign economic aggression.

To launch the initiative, Assistant Attorney General Demers will convene a meeting of the above-mentioned U.S. Attorneys, senior FBI officials, and his counterpart in the Criminal Division, Assistant Attorney General Brian Benczkowski.

###

18-1436
§ 78dd-1. Prohibited foreign trade practices by issuers, 15 USCA § 78dd-1

United States Code Annotated
Title 15. Commerce and Trade
Chapter 2B. Securities Exchanges (Refs & Annos)

15 U.S.C.A. § 78dd-1

§ 78dd-1. Prohibited foreign trade practices by issuers

Effective: November 10, 1998

(a) Prohibition

It shall be unlawful for any issuer which has a class of securities registered pursuant to section 78l of this title or which is required to file reports under section 78a(d) of this title, or for any officer, director, employee, or agent of such issuer or any stockholder thereof acting on behalf of such issuer, to make use of the mails or any means or instrumentality of interstate commerce corruptly in furtherance of an offer, payment, promise to pay, or authorization of the payment of any money, or offer, gift, promise to give, or authorization of the giving of anything of value to--

(1) any foreign official for purposes of--

(A)(i) influencing any act or decision of such foreign official in his official capacity, (ii) inducing such foreign official to do or omit to do any act in violation of the lawful duty of such official, or (iii) securing any improper advantage; or

(B) inducing such foreign official to use his influence with a foreign government or instrumentality thereof to affect or influence any act or decision of such government or instrumentality,

in order to assist such issuer in obtaining or retaining business for or with, or directing business to, any person;

(2) any foreign political party or official thereof or any candidate for foreign political office for purposes of--

(A)(i) influencing any act or decision of such party, official, or candidate in its or his official capacity, (ii) inducing such party, official, or candidate to do or omit to do an act in violation of the lawful duty of such party, official, or candidate, or (iii) securing any improper advantage; or

(B) inducing such party, official, or candidate to use its or his influence with a foreign government or instrumentality thereof to affect or influence any act or decision of such government or instrumentality,

in order to assist such issuer in obtaining or retaining business for or with, or directing business to, any person; or
(3) any person, while knowing that all or a portion of such money or thing of value will be offered, given, or promised, directly or indirectly, to any foreign official, to any foreign political party or official thereof, or to any candidate for foreign political office, for purposes of--

(A)(i) influencing any act or decision of such foreign official, political party, party official, or candidate in his or its official capacity, (ii) inducing such foreign official, political party, party official, or candidate to do or omit to do any act in violation of the lawful duty of such foreign official, political party, party official, or candidate, or (iii) securing any improper advantage; or

(B) inducing such foreign official, political party, party official, or candidate to use his or its influence with a foreign government or instrumentality thereof to affect or influence any act or decision of such government or instrumentality, in order to assist such issuer in obtaining or retaining business for or with, or directing business to, any person.

(b) Exception for routine governmental action

Subsections (a) and (g) shall not apply to any facilitating or expediting payment to a foreign official, political party, or party official the purpose of which is to expedite or to secure the performance of a routine governmental action by a foreign official, political party, or party official.

(c) Affirmative defenses

It shall be an affirmative defense to actions under subsection (a) or (g) that--

(1) the payment, gift, offer, or promise of anything of value that was made, was lawful under the written laws and regulations of the foreign official's, political party's, party official's, or candidate's country; or

(2) the payment, gift, offer, or promise of anything of value that was made, was a reasonable and bona fide expenditure, such as travel and lodging expenses, incurred by or on behalf of a foreign official, party, party official, or candidate and was directly related to--

(A) the promotion, demonstration, or explanation of products or services; or

(B) the execution or performance of a contract with a foreign government or agency thereof.

(d) Guidelines by Attorney General

Not later than one year after August 23, 1988, the Attorney General, after consultation with the Commission, the Secretary of Commerce, the United States Trade Representative, the Secretary of State, and the Secretary of the Treasury, and after obtaining the views of all interested persons through public notice and comment procedures, shall determine to what extent compliance with this section would be enhanced and the business community would be assisted by further clarification of the preceding provisions of this section and may, based on such determination and to the extent necessary and appropriate, issue--
(1) guidelines describing specific types of conduct, associated with common types of export sales arrangements and business contracts, which for purposes of the Department of Justice's present enforcement policy, the Attorney General determines would be in conformance with the preceding provisions of this section; and

(2) general precautionary procedures which issuers may use on a voluntary basis to conform their conduct to the Department of Justice's present enforcement policy regarding the preceding provisions of this section.

The Attorney General shall issue the guidelines and procedures referred to in the preceding sentence in accordance with the provisions of subchapter II of chapter 5 of Title 5 and those guidelines and procedures shall be subject to the provisions of chapter 7 of that title.

(e) Opinions of Attorney General

(1) The Attorney General, after consultation with appropriate departments and agencies of the United States and after obtaining the views of all interested persons through public notice and comment procedures, shall establish a procedure to provide responses to specific inquiries by issuers concerning conformance of their conduct with the Department of Justice's present enforcement policy regarding the preceding provisions of this section. The Attorney General shall, within 30 days after receiving such a request, issue an opinion in response to that request. The opinion shall state whether or not certain specified prospective conduct would, for purposes of the Department of Justice's present enforcement policy, violate the preceding provisions of this section. Additional requests for opinions may be filed with the Attorney General regarding other specified prospective conduct that is beyond the scope of conduct specified in previous requests. In any action brought under the applicable provisions of this section, there shall be a rebuttable presumption that conduct, which is specified in a request by an issuer and for which the Attorney General has issued an opinion that such conduct is in conformity with the Department of Justice's present enforcement policy, is in compliance with the preceding provisions of this section. Such a presumption may be rebutted by a preponderance of the evidence. In considering the presumption for purposes of this paragraph, a court shall weigh all relevant factors, including but not limited to whether the information submitted to the Attorney General was accurate and complete and whether it was within the scope of the conduct specified in any request received by the Attorney General. The Attorney General shall establish the procedure required by this paragraph in accordance with the provisions of subchapter II of chapter 5 of Title 5 and that procedure shall be subject to the provisions of chapter 7 of that title.

(2) Any document or other material which is provided to, received by, or prepared in the Department of Justice or any other department or agency of the United States in connection with a request by an issuer under the procedure established under paragraph (1), shall be exempt from disclosure under section 552 of Title 5 and shall not, except with the consent of the issuer, be made publicly available, regardless of whether the Attorney General responds to such a request or the issuer withdraws such request before receiving a response.

(3) Any issuer who has made a request to the Attorney General under paragraph (1) may withdraw such request prior to the time the Attorney General issues an opinion in response to such request. Any request so withdrawn shall have no force or effect.

(4) The Attorney General shall, to the maximum extent practicable, provide timely guidance concerning the Department of Justice's present enforcement policy with respect to the preceding provisions of this section to potential exporters and small businesses that are unable to obtain specialized counsel on issues pertaining to such provisions. Such guidance shall be limited to responses to requests under paragraph (1) concerning conformity of specified prospective conduct with the Department of
Justice's present enforcement policy regarding the preceding provisions of this section and general explanations of compliance responsibilities and of potential liabilities under the preceding provisions of this section.

(f) Definitions

For purposes of this section:

(1)(A) The term “foreign official” means any officer or employee of a foreign government or any department, agency, or instrumentality thereof, or of a public international organization, or any person acting in an official capacity for or on behalf of any such government or department, agency, or instrumentality, or for or on behalf of any such public international organization.

(B) For purposes of subparagraph (A), the term “public international organization” means--

(i) an organization that is designated by Executive order pursuant to section 288 of Title 22; or

(ii) any other international organization that is designated by the President by Executive order for the purposes of this section, effective as of the date of publication of such order in the Federal Register.

(2)(A) A person's state of mind is “knowing” with respect to conduct, a circumstance, or a result if--

(i) such person is aware that such person is engaging in such conduct, that such circumstance exists, or that such result is substantially certain to occur; or

(ii) such person has a firm belief that such circumstance exists or that such result is substantially certain to occur.

(B) When knowledge of the existence of a particular circumstance is required for an offense, such knowledge is established if a person is aware of a high probability of the existence of such circumstance, unless the person actually believes that such circumstance does not exist.

(3)(A) The term “routine governmental action” means only an action which is ordinarily and commonly performed by a foreign official in--

(i) obtaining permits, licenses, or other official documents to qualify a person to do business in a foreign country;

(ii) processing governmental papers, such as visas and work orders;

(iii) providing police protection, mail pick-up and delivery, or scheduling inspections associated with contract performance or inspections related to transit of goods across country;
(iv) providing phone service, power and water supply, loading and unloading cargo, or protecting perishable products or commodities from deterioration; or

(v) actions of a similar nature.

(B) The term “routine governmental action” does not include any decision by a foreign official whether, or on what terms, to award new business to or to continue business with a particular party, or any action taken by a foreign official involved in the decision-making process to encourage a decision to award new business to or continue business with a particular party.

(g) Alternative jurisdiction

(1) It shall also be unlawful for any issuer organized under the laws of the United States, or a State, territory, possession, or commonwealth of the United States or a political subdivision thereof and which has a class of securities registered pursuant to section 78l of this title or which is required to file reports under section 78o(d) of this title, or for any United States person that is an officer, director, employee, or agent of such issuer or a stockholder thereof acting on behalf of such issuer, to corruptly do any act outside the United States in furtherance of an offer, payment, promise to pay, or authorization of the payment of any money, or offer, gift, promise to give, or authorization of the giving of anything of value to any of the persons or entities set forth in paragraphs (1), (2), and (3) of subsection (a) of this section for the purposes set forth therein, irrespective of whether such issuer or such officer, director, employee, agent, or stockholder makes use of the mails or any means or instrumentality of interstate commerce in furtherance of such offer, gift, payment, promise, or authorization.

(2) As used in this subsection, the term “United States person” means a national of the United States (as defined in section 1101 of Title 8) or any corporation, partnership, association, joint-stock company, business trust, unincorporated organization, or sole proprietorship organized under the laws of the United States or any State, territory, possession, or commonwealth of the United States, or any political subdivision thereof.

CREDIT(S)


EXECUTIVE ORDERS

EXECUTIVE ORDER NO. 13259

<March 19, 2002, 67 F.R. 13239>

ORGANIZATIONS FOR PURPOSES OF THE SECURITIES EXCHANGE ACT OF 1934 AND THE FOREIGN CORRUPT PRACTICES ACT OF 1977

§ 78dd-1. Prohibited foreign trade practices by issuers, 15 USCA § 78dd-1

Designate as “public international organizations” for the purposes of application of section 30A of the Securities Exchange Act of 1934 and sections 104 and 104A of the Foreign Corrupt Practices Act of 1977:

(a) The European Union, including: the European Communities (the European Community, the European Coal & Steel Community, and the European Atomic Energy Community); institutions of the European Union, such as the European Commission, the Council of the European Union, the European Parliament, the European Court of Justice, the European Court of Auditors, the Economic and Social Committee, the Committee of the Regions, the European Central Bank, and the European Investment Bank; and any departments, agencies, and instrumentalities thereof; and

(b) The European Police Office (Europol), including any departments, agencies, and instrumentalities thereof.

Designation in this Executive Order is intended solely to further the purposes of the statutes mentioned above and is not determinative of whether an entity is a public international organization for the purpose of other statutes or regulations.

GEORGE W. BUSH

MEMORANDA OF PRESIDENT

Delegation of Authority Under Section 5(d)(2) of the International Anti-Bribery and Fair Competition Act of 1998

Memoranda of President, Nov. 16, 1998, 63 F.R. 65997, delegated to the Secretary of State the functions and authorities vested in the President by section 5(d)(2) of the International Anti-Bribery and Fair Competition Act of 1998 (Public Law 105-366).

Notes of Decisions (35)

15 U.S.C.A. § 78dd-1, 15 USCA § 78dd-1
Current through P.L. 116-47.

EXECUTIVE ORDERS

EXECUTIVE ORDER NO. 9176

<May 29, 1942, 7 F.R. 4127>

Transfer of Registration Functions from the Secretary of State to the Attorney General

By virtue of the authority vested in me by Title I of the First War Powers Act, 1941, approved December 18, 1941 (Public Law No. 354, 77th Congress [section 601 et seq. of the former Appendix to Title 50, War and National Defense] ), and as President of the United States, it is hereby ordered as follows:

1. All functions, powers and duties of the Secretary of State under the act of June 8, 1938 (52 Stat. 631), as amended by the act of August 7, 1939 (53 Stat. 1244) [this subchapter], requiring the registration of agents of foreign principals, are hereby transferred to and vested in the Attorney General.

2. All property, books and records heretofore maintained by the Secretary of State with respect to his administration of said act of June 8, 1938, as amended, are hereby transferred to and vested in the Attorney General.

3. The Attorney General shall furnish to the Secretary of State for such comment, if any, as the Secretary of State may desire to make from the point of view of the foreign relations of the United States, one copy of each registration statement that is hereafter filed with the Attorney General in accordance with the provisions of this Executive order.

4. All rules, regulations and forms which have been issued by the Secretary of State pursuant to the provisions of said act of June 8, 1938, as amended, and which are in effect shall continue in effect until modified, superseded, revoked or repealed by the Attorney General.

5. This order shall become effective as of June 1, 1942.
United States Code Annotated
Title 22. Foreign Relations and Intercourse
Chapter 11. Foreign Agents and Propaganda
Subchapter II. Registration of Foreign Propagandists (Refs & Annos)

22 U.S.C.A. § 611
§ 611. Definitions

Currentness

As used in and for the purposes of this subchapter--

(a) The term “person” includes an individual, partnership, association, corporation, organization, or any other combination of individuals;

(b) The term “foreign principal” includes--

(1) a government of a foreign country and a foreign political party;

(2) a person outside of the United States, unless it is established that such person is an individual and a citizen of and domiciled within the United States, or that such person is not an individual and is organized under or created by the laws of the United States or of any State or other place subject to the jurisdiction of the United States and has its principal place of business within the United States; and

(3) a partnership, association, corporation, organization, or other combination of persons organized under the laws of or having its principal place of business in a foreign country.

(c) Expect as provided in subsection (d) of this section, the term “agent of a foreign principal” means--

(1) any person who acts as an agent, representative, employee, or servant, or any person who acts in any other capacity at the order, request, or under the direction or control, of a foreign principal or of a person any of whose activities are directly or indirectly supervised, directed, controlled, financed, or subsidized in whole or in major part by a foreign principal, and who directly or through any other person--

(i) engages within the United States in political activities for or in the interests of such foreign principal;

(ii) acts within the United States as a public relations counsel, publicity agent, information-service employee or political consultant for or in the interests of such foreign principal;
(iii) within the United States solicits, collects, disburses, or dispenses contributions, loans, money, or other things of value for or in the interest of such foreign principal; or

(iv) within the United States represents the interests of such foreign principal before any agency or official of the Government of the United States; and

(2) any person who agrees, consents, assumes or purports to act as, or who is or holds himself out to be, whether or not pursuant to contractual relationship, an agent of a foreign principal as defined in clause (1) of this subsection.

(d) The term “agent of a foreign principal” does not include any news or press service or association organized under the laws of the United States or of any State or other place subject to the jurisdiction of the United States, or any newspaper, magazine, periodical, or other publication for which there is on file with the United States Postal Service information in compliance with section 3611 of Title 39, published in the United States, solely by virtue of any bona fide news or journalistic activities, including the solicitation or acceptance of advertisements, subscriptions, or other compensation therefor, so long as it is at least 80 per centum beneficially owned by, and its officers and directors, if any, are citizens of the United States, and such news or press service or association, newspaper, magazine, periodical, or other publication, is not owned, directed, supervised, controlled, subsidized, or financed, and none of its policies are determined by any foreign principal defined in subsection (b) of this section, or by any agent of a foreign principal required to register under this subchapter;

(e) The term “government of a foreign country” includes any person or group of persons exercising sovereign de facto or de jure political jurisdiction over any country, other than the United States, or over any part of such country, and includes any subdivision of any such group and any group or agency to which such sovereign de facto or de jure authority or functions are directly or indirectly delegated. Such term shall include any faction or body of insurgents within a country assuming to exercise governmental authority whether such faction or body of insurgents has or has not been recognized by the United States;

(f) The term “foreign political party” includes any organization or any other combination of individuals in a country other than the United States, or any unit or branch thereof, having for an aim or purpose, or which is engaged in any activity devoted in whole or in part to, the establishment, administration, control, or acquisition of administration or control, of a government of a foreign country or a subdivision thereof, or the furtherance or influencing of the political or public interests, policies, or relations of a government of a foreign country or a subdivision thereof;

(g) The term “public-relations counsel” includes any person who engages directly or indirectly in informing, advising, or in any way representing a principal in any public relations matter pertaining to political or public interests, policies, or relations of such principal;

(h) The term “publicity agent” includes any person who engages directly or indirectly in the publication or dissemination of oral, visual, graphic, written, or pictorial information or matter of any kind, including publication by means of advertising, books, periodicals, newspapers, lectures, broadcasts, motion pictures, or otherwise;

(i) The term “information-service employee” includes any person who is engaged in furnishing, disseminating, or publishing accounts, descriptions, information, or data with respect to the political, industrial, employment, economic, social, cultural,
or other benefits, advantages, facts, or conditions of any country other than the United States or of any government of a foreign country or of a foreign political party or of a partnership, association, corporation, organization, or other combination of individuals organized under the laws of, or having its principal place of business in, a foreign country;


(k) The term “registration statement” means the registration statement required to be filed with the Attorney General under section 612(a) of this title, and any supplements thereto required to be filed under section 612(b) of this title, and includes all documents and papers required to be filed therewith or amendatory thereof or supplemental thereto, whether attached thereto or incorporated therein by reference;

(l) The term “American republic” includes any of the states which were signatory to the Final Act of the Second Meeting of the Ministers of Foreign Affairs of the American Republics at Habana, Cuba, July 30, 1940;

(m) The term “United States”, when used in a geographical sense, includes the several States, the District of Columbia, the Territories, the Canal Zone, the insular possessions, and all other places now or hereafter subject to the civil or military jurisdiction of the United States;

(n) The term “prints” means newspapers and periodicals, books, pamphlets, sheet music, visiting cards, address cards, printing proofs, engravings, photographs, pictures, drawings, plans, maps, patterns to be cut out, catalogs, prospectuses, advertisements, and printed, engraved, lithographed, or autographed notices of various kinds, and, in general, all impressions or reproductions obtained on paper or other material assimilable to paper, on parchment or on cardboard, by means of printing, engraving, lithography, autography, or any other easily recognizable mechanical process, with the exception of the copying press, stamps with movable or immovable type, and the typewriter;

(o) The term “political activities” means any activity that the person engaging in believes will, or that the person intends to, in any way influence any agency or official of the Government of the United States or any section of the public within the United States with reference to formulating, adopting, or changing the domestic or foreign policies of the United States or with reference to the political or public interests, policies, or relations of a government of a foreign country or a foreign political party;

(p) The term “political consultant” means any person who engages in informing or advising any other person with reference to the domestic or foreign policies of the United States or the political or public interest, policies, or relations of a foreign country or of a foreign political party.

CREDIT(S)

Notes of Decisions (19)

Footnotes
1 So in original. Probably should be “Except”.
2 So in original. Probably should be “section 3685”.

22 U.S.C.A. § 611, 22 USCA § 611
Current through P.L. 116-47.
§ 612. Registration statement, 22 USCA § 612

United States Code Annotated
Title 22. Foreign Relations and Intercourse
Chapter 11. Foreign Agents and Propaganda
Subchapter II. Registration of Foreign Propagandists (Refs & Annos)

22 U.S.C.A. § 612

§ 612. Registration statement

Currentness

(a) Filing; contents

No person shall act as an agent of a foreign principal unless he has filed with the Attorney General a true and complete registration statement and supplements thereto as required by subsections (a) and (b) of this section or unless he is exempt from registration under the provisions of this subchapter. Except as hereinafter provided, every person who becomes an agent of a foreign principal shall, within ten days thereafter, file with the Attorney General, in duplicate, a registration statement, under oath on a form prescribed by the Attorney General. The obligation of an agent of a foreign principal to file a registration statement shall, after the tenth day of his becoming such agent, continue from day to day, and termination of such status shall not relieve such agent from his obligation to file a registration statement for the period during which he was an agent of a foreign principal. The registration statement shall include the following, which shall be regarded as material for the purposes of this subchapter:

(1) Registrant's name, principal business address, and all other business addresses in the United States or elsewhere, and all residence addresses, if any;

(2) Status of the registrant; if an individual, nationality; if a partnership, name, residence addresses, and nationality of each partner and a true and complete copy of its articles of copartnership; if an association, corporation, organization, or any other combination of individuals, the name, residence addresses, and nationality of each director and officer and of each person performing the functions of a director or officer and a true and complete copy of its charter, articles of incorporation, association, constitution, and bylaws, and amendments thereto; a copy of every other instrument or document and a statement of the terms and conditions of every oral agreement relating to its organization, powers, and purposes; and a statement of its ownership and control;

(3) A comprehensive statement of the nature of registrant's business; a complete list of registrant's employees and a statement of the nature of the work of each; the name and address of every foreign principal for whom the registrant is acting, assuming or purporting to act or has agreed to act; the character of the business or other activities of every such foreign principal, and, if any such foreign principal be other than a natural person, a statement of the ownership and control of each; and the extent, if any, to which each such foreign principal is supervised, directed, owned, controlled, financed, or subsidized, in whole or in part, by any government of a foreign country or foreign political party, or by any other foreign principal;

(4) Copies of each written agreement and the terms and conditions of each oral agreement, including all modifications of such agreements, or, where no contract exists, a full statement of all the circumstances, by reason of which the registrant is
an agent of a foreign principal; a comprehensive statement of the nature and method of performance of each such contract, and of the existing and proposed activity or activities engaged in or to be engaged in by the registrant as agent of a foreign principal for each such foreign principal, including a detailed statement of any such activity which is a political activity;

(5) The nature and amount of contributions, income, money, or thing of value, if any, that the registrant has received within the preceding sixty days from each such foreign principal, either as compensation or for disbursement or otherwise, and the form and time of each such payment and from whom received;

(6) A detailed statement of every activity which the registrant is performing or is assuming or purporting or has agreed to perform for himself or any other person other than a foreign principal and which requires his registration hereunder, including a detailed statement of any such activity which is a political activity;

(7) The name, business, and residence addresses, and if an individual, the nationality, of any person other than a foreign principal for whom the registrant is acting, assuming or purporting to act or has agreed to act under such circumstances as require his registration hereunder; the extent to which each such person is supervised, directed, owned, controlled, financed, or subsidized, in whole or in part, by any government of a foreign country or foreign political party or by any other foreign principal; and the nature and amount of contributions, income, money, or thing of value, if any, that the registrant has received during the preceding sixty days from each such person in connection with any of the activities referred to in clause (6) of this subsection, either as compensation or for disbursement or otherwise, and the form and time of each such payment and from whom received;

(8) A detailed statement of the money and other things of value spent or disposed of by the registrant during the preceding sixty days in furtherance of or in connection with activities which require his registration hereunder and which have been undertaken by him either as an agent of a foreign principal or for himself or any other person or in connection with any activities relating to his becoming an agent of such principal, and a detailed statement of any contributions of money or other things of value made by him during the preceding sixty days (other than contributions the making of which is prohibited under the terms of section 613 of Title 18) in connection with an election to any political office or in connection with any primary election, convention, or caucus held to select candidates for any political office;

(9) Copies of each written agreement and the terms and conditions of each oral agreement, including all modifications of such agreements, or, where no contract exists, a full statement of all the circumstances, by reason of which the registrant is performing or assuming or purporting or has agreed to perform for himself or for a foreign principal or for any person other than a foreign principal any activities which require his registration hereunder;

(10) Such other statements, information, or documents pertinent to the purposes of this subchapter as the Attorney General, having due regard for the national security and the public interest, may from time to time require;

(11) Such further statements and such further copies of documents as are necessary to make the statements made in the registration statement and supplements thereto, and the copies of documents furnished therewith, not misleading.

(b) Supplements; filing period
Every agent of a foreign principal who has filed a registration statement required by subsection (a) of this section shall, within thirty days after the expiration of each period of six months succeeding such filing, file with the Attorney General a supplement thereto under oath, on a form prescribed by the Attorney General, which shall set forth with respect to such preceding six months' period such facts as the Attorney General, having due regard for the national security and the public interest, may deem necessary to make the information required under this section accurate, complete, and current with respect to such period. In connection with the information furnished under clauses (3), (4), (6), and (9) of subsection (a) of this section, the registrant shall give notice to the Attorney General of any changes therein within ten days after such changes occur. If the Attorney General, having due regard for the national security and the public interest, determines that it is necessary to carry out the purposes of this subchapter, he may, in any particular case, require supplements to the registration statement to be filed at more frequent intervals in respect to all or particular items of information to be furnished.

(c) Execution of statement under oath

The registration statement and supplements thereto shall be executed under oath as follows: If the registrant is an individual, by him; if the registrant is a partnership, by the majority of the members thereof; if the registrant is a person other than an individual or a partnership, by a majority of the officers thereof or persons performing the functions of officers or by a majority of the board of directors thereof or persons performing the functions of directors, if any.

(d) Filing of statement not deemed full compliance nor as preclusion from prosecution

The fact that a registration statement or supplement thereto has been filed shall not necessarily be deemed a full compliance with this subchapter and the regulations thereunder on the part of the registrant; nor shall it indicate that the Attorney General has in any way passed upon the merits of such registration statement or supplement thereto; nor shall it preclude prosecution, as provided for in this subchapter, for willful failure to file a registration statement or supplement thereto when due or for a willful false statement of a material fact therein or the willful omission of a material fact required to be stated therein or the willful omission of a material fact or copy of a material document necessary to make the statements made in a registration statement and supplements thereto, and the copies of documents furnished therewith, not misleading.

(e) Incorporation of previous statement by reference

If any agent of a foreign principal, required to register under the provisions of this subchapter, has previously thereto registered with the Attorney General under the provisions of section 2386 of Title 18, the Attorney General, in order to eliminate inappropriate duplication, may permit the incorporation by reference in the registration statement or supplements thereto filed hereunder of any information or documents previously filed by such agent of a foreign principal under the provisions of said section.

(f) Exemption by Attorney General

The Attorney General may, by regulation, provide for the exemption--

(1) from registration, or from the requirement of furnishing any of the information required by this section, of any person who is listed as a partner, officer, director, or employee in the registration statement filed by an agent of a foreign principal under this subchapter, and

(2) from the requirement of furnishing any of the information required by this section of any agent of a foreign principal,
where by reason of the nature of the functions or activities of such person the Attorney General, having due regard for the national security and the public interest, determines that such registration, or the furnishing of such information, as the case may be, is not necessary to carry out the purposes of this subchapter.

(g) Electronic filing of registration statements and supplements

A registration statement or supplement required to be filed under this section shall be filed in electronic form, in addition to any other form that may be required by the Attorney General.

CREDIT(S)


Notes of Decisions (12)

Footnotes

1 So in original. Probably should be “connection”.

22 U.S.C.A. § 612, 22 USCA § 612
Current through P.L. 116-47.
The requirements of section 612(a) of this title shall not apply to the following agents of foreign principals:

(a) **Diplomatic or consular officers**

A duly accredited diplomatic or consular officer of a foreign government who is so recognized by the Department of State, while said officer is engaged exclusively in activities which are recognized by the Department of State as being within the scope of the functions of such officer;

(b) **Officials of foreign government**

Any official of a foreign government, if such government is recognized by the United States, who is not a public-relations counsel, publicity agent, information-service employee, or a citizen of the United States, whose name and status and the character of whose duties as such official are of public record in the Department of State, while said official is engaged exclusively in activities which are recognized by the Department of State as being within the scope of the functions of such official;

(c) **Staff members of diplomatic or consular officers**

Any member of the staff of, or any person employed by, a duly accredited diplomatic or consular officer of a foreign government who is so recognized by the Department of State, other than a public-relations counsel, publicity agent, or information-service employee, whose name and status and the character of whose duties as such member or employee are of public record in the Department of State, while said member or employee is engaged exclusively in the performance of activities which are recognized by the Department of State as being within the scope of the functions of such member or employee;

(d) **Private and nonpolitical activities; solicitation of funds**

Any person engaging or agreeing to engage only (1) in private and nonpolitical activities in furtherance of the bona fide trade or commerce of such foreign principal; or (2) in other activities not serving predominantly a foreign interest; or (3) in the soliciting or collecting of funds and contributions within the United States to be used only for medical aid and assistance, or for food and clothing to relieve human suffering, if such solicitation or collection of funds and contributions is in accordance with and subject to the provisions of subchapter II of chapter 9 of this title, and such rules and regulations as may be prescribed thereunder;

(e) **Religious, scholastic, or scientific pursuits**
§ 613. Exemptions, 22 USCA § 613

Any person engaging or agreeing to engage only in activities in furtherance of bona fide religious, scholastic, academic, or scientific pursuits or of the fine arts;

(f) Defense of foreign government vital to United States defense

Any person, or employee of such person, whose foreign principal is a government of a foreign country the defense of which the President deems vital to the defense of the United States while, (1) such person or employee engages only in activities which are in furtherance of the policies, public interest, or national defense both of such government and of the Government of the United States, and are not intended to conflict with any of the domestic or foreign policies of the Government of the United States, (2) each communication or expression by such person or employee which he intends to, or has reason to believe will, be published, disseminated, or circulated among any section of the public, or portion thereof, within the United States, is a part of such activities and is believed by such person to be truthful and accurate and the identity of such person as an agent of such foreign principal is disclosed therein, and (3) such government of a foreign country furnishes to the Secretary of State for transmittal to, and retention for the duration of this subchapter by, the Attorney General such information as to the identity and activities of such person or employee at such times as the Attorney General may require. Upon notice to the Government of which such person is an agent or to such person or employee, the Attorney General, having due regard for the public interest and national defense, may, with the approval of the Secretary of State, and shall, at the request of the Secretary of State, terminate in whole or in part the exemption herein of any such person or employee;

(g) Persons qualified to practice law

Any person qualified to practice law, insofar as he engages or agrees to engage in the legal representation of a disclosed foreign principal before any court of law or any agency of the Government of the United States: Provided, That for the purposes of this subsection legal representation does not include attempts to influence or persuade agency personnel or officials other than in the course of judicial proceedings, criminal or civil law enforcement inquiries, investigations, or proceedings, or agency proceedings required by statute or regulation to be conducted on the record.

(h) Agents of foreign principals

Any agent of a person described in section 611(b)(2) of this title or an entity described in section 611(b)(3) of this title if the agent has engaged in lobbying activities and has registered under the Lobbying Disclosure Act of 1995 in connection with the agent's representation of such person or entity.

CREDIT(S)


Notes of Decisions (5)

22 U.S.C.A. § 613, 22 USCA § 613
Current through P.L. 116-47.
§ 614. Filing and labeling of political propaganda, 22 USCA § 614

(a) Copies to Attorney General; statement as to places, times, and extent of transmission

Every person within the United States who is an agent of a foreign principal and required to register under the provisions of this subchapter and who transmits or causes to be transmitted in the United States mails or by any means or instrumentality of interstate or foreign commerce any informational materials for or in the interests of such foreign principal (i) in the form of prints, or (ii) in any other form which is reasonably adapted to being, or which he believes will be, or which he intends to be, disseminated or circulated among two or more persons shall, not later than forty-eight hours after the beginning of the transmittal thereof, file with the Attorney General two copies thereof.

(b) Identification statement

It shall be unlawful for any person within the United States who is an agent of a foreign principal and required to register under the provisions of this subchapter to transmit or cause to be transmitted in the United States mails or by any means or instrumentality of interstate or foreign commerce any informational materials for or in the interests of such foreign principal without placing in such informational materials a conspicuous statement that the materials are distributed by the agent on behalf of the foreign principal, and that additional information is on file with the Department of Justice, Washington, District of Columbia. The Attorney General may by rule define what constitutes a conspicuous statement for the purposes of this subsection.

(c) Public inspection

The copies of informational materials required by this subchapter to be filed with the Attorney General shall be available for public inspection under such regulations as he may prescribe.

(d) Library of Congress

For purposes of the Library of Congress, other than for public distribution, the Secretary of the Treasury and the United States Postal Service are authorized, upon the request of the Librarian of Congress, to forward to the Library of Congress fifty copies, or as many fewer thereof as are available, of all foreign prints determined to be prohibited entry under the provisions of section 1305 of Title 19 and of all foreign prints excluded from the mails under authority of section 1717 of Title 18.

Notwithstanding the provisions of section 1305 of Title 19 and of section 1717 of Title 18, the Secretary of the Treasury is authorized to permit the entry and the United States Postal Service is authorized to permit the transmittal in the mails of foreign

\[\text{Currentness}\]
prints imported for governmental purposes by authority or for the use of the United States or for the use of the Library of Congress.

(e) Information furnished to agency or official of United States Government

It shall be unlawful for any person within the United States who is an agent of a foreign principal required to register under the provisions of this subchapter to transmit, convey, or otherwise furnish to any agency or official of the Government (including a Member or committee of either House of Congress) for or in the interests of such foreign principal any political propaganda or to request from any such agency or official for or in the interests of such foreign principal any information or advice with respect to any matter pertaining to the political or public interests, policies or relations of a foreign country or of a political party or pertaining to the foreign or domestic policies of the United States unless the propaganda or the request is prefaced or accompanied by a true and accurate statement to the effect that such person is registered as an agent of such foreign principal under this subchapter.

(f) Appearances before Congressional committees

Whenever any agent of a foreign principal required to register under this subchapter appears before any committee of Congress to testify for or in the interests of such foreign principal, he shall, at the time of such appearance, furnish the committee with a copy of his most recent registration statement filed with the Department of Justice as an agent of such foreign principal for inclusion in the records of the committee as part of his testimony.

CREDIT(S)


22 U.S.C.A. § 614, 22 USCA § 614
Current through P.L. 116-47.
§ 615. Books and records

22 U.S.C.A. § 615

§ 615. Books and records

Currentness

Every agent of a foreign principal registered under this subchapter shall keep and preserve while he is an agent of a foreign principal such books of account and other records with respect to all his activities, the disclosure of which is required under the provisions of this subchapter, in accordance with such business and accounting practices, as the Attorney General, having due regard for the national security and the public interest, may by regulation prescribe as necessary or appropriate for the enforcement of the provisions of this subchapter and shall preserve the same for a period of three years following the termination of such status. Until regulations are in effect under this section every agent of a foreign principal shall keep books of account and shall preserve all written records with respect to his activities. Such books and records shall be open at all reasonable times to the inspection of any official charged with the enforcement of this subchapter. It shall be unlawful for any person willfully to conceal, destroy, obliterate, mutilate, or falsify, or to attempt to conceal, destroy, obliterate, mutilate, or falsify, or to cause to be concealed, destroyed, obliterated, mutilated, or falsified, any books or records required to be kept under the provisions of this section.

CREDIT(S)


Notes of Decisions (5)

22 U.S.C.A. § 615, 22 USCA § 615
Current through P.L. 116-47.

End of Document
§ 616. Public examination of official records; transmittal of records and information

Currentness

(a) Permanent copy of statement; inspection; withdrawal

The Attorney General shall retain in permanent form one copy of all registration statements furnished under this subchapter, and the same shall be public records and open to public examination and inspection at such reasonable hours, under such regulations, as the Attorney General may prescribe, and copies of the same shall be furnished to every applicant at such reasonable fee as the Attorney General may prescribe. The Attorney General may withdraw from public examination the registration statement and other statements of any agent of a foreign principal whose activities have ceased to be of a character which requires registration under the provisions of this subchapter.

(b) Secretary of State

The Attorney General shall, promptly upon receipt, transmit one copy of every registration statement filed hereunder and one copy of every amendment or supplement thereto filed hereunder, to the Secretary of State for such comment and use as the Secretary of State may determine to be appropriate from the point of view of the foreign relations of the United States. Failure of the Attorney General so to transmit such copy shall not be a bar to prosecution under this subchapter.

(c) Executive departments and agencies; Congressional committees

The Attorney General is authorized to furnish to departments and agencies in the executive branch and committees of the Congress such information obtained by him in the administration of this subchapter, including the names of registrants under this subchapter, copies of registration statements, or parts thereof, or other documents or information filed under this subchapter, as may be appropriate in the light of the purposes of this subchapter.

(d) Public database of registration statements and updates

(1) In general

The Attorney General shall maintain, and make available to the public over the Internet, without a fee or other access charge, in a searchable, sortable, and downloadable manner, to the extent technically practicable, an electronic database that--
(A) includes the information contained in registration statements and updates filed under this subchapter; and

(B) is searchable and sortable, at a minimum, by each of the categories of information described in section 612(a) of this title.

(2) Accountability

The Attorney General shall make each registration statement and update filed in electronic form pursuant to section 612(g) of this title available for public inspection over the Internet as soon as technically practicable after the registration statement or update is filed.

CREDIT(S)


Notes of Decisions (1)

22 U.S.C.A. § 616, 22 USCA § 616
Current through P.L. 116-47.
§ 617. Liability of officers

Each officer, or person performing the functions of an officer, and each director, or person performing the functions of a director, of an agent of a foreign principal which is not an individual shall be under obligation to cause such agent to execute and file a registration statement and supplements thereto as and when such filing is required under subSections (a) and (b) of section 612 of this title and shall also be under obligation to cause such agent to comply with all the requirements of sections 614(a) and (b) and 615 of this title and all other requirements of this subchapter. Dissolution of any organization acting as an agent of a foreign principal shall not relieve any officer, or person performing the functions of an officer, or any director, or person performing the functions of a director, from complying with the provisions of this section. In case of failure of any such agent of a foreign principal to comply with any of the requirements of this subchapter, each of its officers, or persons performing the functions of officers, and each of its directors, or persons performing the functions of directors, shall be subject to prosecution therefor.

CREDIT(S)

(June 8, 1938, c. 327, § 7, 52 Stat. 633; Apr. 29, 1942, c. 263, § 1, 56 Stat. 256; Aug. 3, 1950, c. 524, § 2, 64 Stat. 400.)

22 U.S.C.A. § 617, 22 USCA § 617
Current through P.L. 116-47.
United States Code Annotated
Title 22. Foreign Relations and Intercourse
Chapter 11. Foreign Agents and Propaganda
Subchapter II. Registration of Foreign Propagandists (Refs & Annos)

22 U.S.C.A. § 618

§ 618. Enforcement and penalties

Effective: June 5, 2004

Currentness

(a) Violations; false statements and willful omissions

Any person who--

(1) willfully violates any provision of this subchapter or any regulation thereunder, or

(2) in any registration statement or supplement thereto or in any other document filed with or furnished to the Attorney General under the provisions of this subchapter willfully makes a false statement of a material fact or willfully omits any material fact required to be stated therein or willfully omits a material fact or a copy of a material document necessary to make the statements therein and the copies of documents furnished therewith not misleading, shall, upon conviction thereof, be punished by a fine of not more than $10,000 or by imprisonment for not more than five years, or both, except that in the case of a violation of subsection (b), (e), or (f) of section 614 of this title or of subsection (g) or (h) of this section the punishment shall be a fine of not more than $5,000 or imprisonment for not more than six months, or both.

(b) Proof of identity of foreign principal

In any proceeding under this subchapter in which it is charged that a person is an agent of a foreign principal with respect to a foreign principal outside of the United States, proof of the specific identity of the foreign principal shall be permissible but not necessary.

(c) Removal

Any alien who shall be convicted of a violation of, or a conspiracy to violate, any provision of this subchapter or any regulation thereunder shall be subject to removal pursuant to chapter 4 of title II of the Immigration and Nationality Act.


(e) Continuing offense
§ 618. Enforcement and penalties, 22 USCA § 618

Failure to file any such registration statement or supplements thereto as is required by either section 612(a) or section 612(b) of this title shall be considered a continuing offense for as long as such failure exists, notwithstanding any statute of limitation or other statute to the contrary.

(f) Injunctive remedy; jurisdiction of district court

Whenever in the judgment of the Attorney General any person is engaged in or about to engage in any acts which constitute or will constitute a violation of any provision of this subchapter, or regulations issued thereunder, or whenever any agent of a foreign principal fails to comply with any of the provisions of this subchapter or the regulations issued thereunder, or otherwise is in violation of the subchapter, the Attorney General may make application to the appropriate United States district court for an order enjoining such acts or enjoining such person from continuing to act as an agent of such foreign principal, or for an order requiring compliance with any appropriate provision of the subchapter or regulation thereunder. The district court shall have jurisdiction and authority to issue a temporary or permanent injunction, restraining order or such other order which it may deem proper.

(g) Deficient registration statement

If the Attorney General determines that a registration statement does not comply with the requirements of this subchapter or the regulations issued thereunder, he shall so notify the registrant in writing, specifying in what respects the statement is deficient. It shall be unlawful for any person to act as an agent of a foreign principal at any time ten days or more after receipt of such notification without filing an amended registration statement in full compliance with the requirements of this subchapter and the regulations issued thereunder.

(h) Contingent fee arrangement

It shall be unlawful for any agent of a foreign principal required to register under this subchapter to be a party to any contract, agreement, or understanding, either express or implied, with such foreign principal pursuant to which the amount or payment of the compensation, fee, or other remuneration of such agent is contingent in whole or in part upon the success of any political activities carried on by such agent.

CREDIT(S)


Notes of Decisions (17)

22 U.S.C.A. § 618, 22 USCA § 618
Current through P.L. 116-47.
§ 619. Territorial applicability of subchapter, 22 USCA § 619

This subchapter shall be applicable in the several States, the District of Columbia, the Territories, the Canal Zone, the insular possessions, and all other places now or hereafter subject to the civil or military jurisdiction of the United States.

CREDIT(S)

(June 8, 1938, c. 327, § 9, as added Apr. 29, 1942, c. 263, § 1, 56 Stat. 257; amended Proc. No. 2695, July 4, 1946, 11 F.R. 7517, 60 Stat. 1352.)

22 U.S.C.A. § 619, 22 USCA § 619
Current through P.L. 116-47.
§ 620. Rules and regulations, 22 USCA § 620

United States Code Annotated
Title 22. Foreign Relations and Intercourse
Chapter 11. Foreign Agents and Propaganda
Subchapter II. Registration of Foreign Propagandists (Refs & Annos)

22 U.S.C.A. § 620

§ 620. Rules and regulations

Currentness

The Attorney General may at any time make, prescribe, amend, and rescind such rules, regulations, and forms as he may deem necessary to carry out the provisions of this subchapter.

CREDIT(S)

(June 8, 1938, c. 327, § 10, as added Apr. 29, 1942, c. 263, § 1, 56 Stat. 257.)

22 U.S.C.A. § 620, 22 USCA § 620
Current through P.L. 116-47.

End of Document
§ 621. Reports to Congress

Currentness

The Attorney General shall every six months report to the Congress concerning administration of this subchapter, including registrations filed pursuant to the subchapter, and the nature, sources and content of political propaganda disseminated and distributed.

CREDIT(S)


22 U.S.C.A. § 621, 22 USCA § 621
Current through P.L. 116-47.
§ 1832. Theft of trade secrets, 18 USCA § 1832

(a) Whoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly--

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;

(3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

(4) attempts to commit any offense described in paragraphs (1) through (3); or

(5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,

shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

(b) Any organization that commits any offense described in subsection (a) shall be fined not more than the greater of $5,000,000 or 3 times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided.

CREDIT(S)

Notes of Decisions (16)

18 U.S.C.A. § 1832, 18 USCA § 1832
Current through P.L. 116-47.
UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA
- against -

HUAWEI TECHNOLOGIES CO., LTD.,
HUAWEI DEVICE USA INC.,
SKYCOM TECH CO. LTD.,
WANZHOU MENG,
also known as "Cathy Meng" and
"Sabrina Meng,"

Defendants.

THE GRAND JURY CHARGES:

INTRODUCTION

At all times relevant to this Superseding Indictment, unless otherwise
indicated:

I. The Defendants

1. The defendant HUAWEI TECHNOLOGIES CO., LTD. ("HUAWEI")

was a global networking, telecommunications and services company headquartered in
Shenzhen, Guangdong, in the People's Republic of China ("PRC"). HUAWEI was owned
by a parent company ("Huawei Parent"), an entity whose identity is known to the Grand
Jury, registered in Shenzhen, Guangdong, in the PRC. As of the date of the filing of this
Superseding Indictment, HUAWEI was the largest telecommunications equipment manufacturer in the world.

2. HUAWEI operated numerous subsidiaries throughout the world, including in the United States. One U.S. subsidiary was the defendant HUAWEI DEVICE USA INC. ("HUAWEI USA"), whose headquarters were in Plano, Texas.

3. The defendant SKYCOM TECH CO. LTD. ("SKYCOM") was a corporation registered in Hong Kong whose primary operations were in Iran. SKYCOM functioned as HUAWEI's Iran-based subsidiary. As of 2007, Huawei Parent owned SKYCOM through a subsidiary ("Huawei Subsidiary 1"), an entity whose identity is known to the Grand Jury. In or about November 2007, Huawei Subsidiary 1 transferred its shares of SKYCOM to another entity ("Huawei Subsidiary 2"), an entity whose identity is known to the Grand Jury, and which was purportedly a third party in the transaction but was actually controlled by HUAWEI. Following this transfer of SKYCOM shares from Huawei Subsidiary 1 to Huawei Subsidiary 2, HUAWEI falsely claimed that SKYCOM was one of HUAWEI's local business partners in Iran, as opposed to one of HUAWEI's subsidiaries or affiliates.

4. The defendant WANZHOU MENG, also known as "Cathy Meng" and "Sabrina Meng," was a citizen of the PRC. From at least in or about 2010, MENG served as Chief Financial Officer of HUAWEI. Between approximately February 2008 and April 2009, MENG served on the SKYCOM Board of Directors. More recently, MENG also served as Deputy Chairwoman of the Board of Directors for HUAWEI.
II. The Victim Financial Institutions

7. Financial Institution 1, an entity whose identity is known to the Grand Jury, was a multinational banking and financial services company, which operated subsidiaries throughout the world, including in the United States and in Eurozone countries. Its United States-based subsidiary ("U.S. Subsidiary 1"), an entity whose identity is known to the Grand Jury, was a federally chartered bank, the deposits of which were insured by the Federal Deposit Insurance Company ("FDIC"). Among the services offered by Financial Institution 1 to its clients were U.S.-dollar clearing through U.S. Subsidiary 1 and other financial institutions located in the United States, and Euro clearing through Financial Institution 1 subsidiaries and other financial institutions located in Eurozone countries. Between approximately 2010 and 2014, Financial Institution 1 and U.S. Subsidiary 1 cleared more than $100 million worth of transactions related to SKYCOM through the United States. In or about 2017, Financial Institution 1 verbally communicated to HUAWEI representatives that it was terminating its banking relationship with HUAWEI.

8. Financial Institution 2, an entity whose identity is known to the Grand Jury, was a multinational banking and financial services company, which operated subsidiaries throughout the world, including in the United States and in Eurozone countries.
Among the services offered by Financial Institution 2 to its clients were U.S.-dollar clearing through a Financial Institution 2 subsidiary and other financial institutions located in the United States, and Euro clearing through Financial Institution 2 subsidiaries and other financial institutions located in Eurozone countries.

9. Financial Institution 3, an entity whose identity is known to the Grand Jury, was a multinational banking and financial services company, which operated subsidiaries throughout the world, including in the United States and in Eurozone countries. Among the services offered by Financial Institution 3 to its clients were U.S.-dollar clearing through Financial Institution 3 subsidiaries and other financial institutions located in the United States, and Euro clearing through Financial Institution 3 subsidiaries and other financial institutions located in Eurozone countries.

10. Financial Institution 4, an entity whose identity is known to the Grand Jury, was a multinational banking and financial services company operating subsidiaries throughout the world, including in the United States and in Eurozone countries. Among the services offered by Financial Institution 4 to its clients were U.S.-dollar clearing through Financial Institution 4 subsidiaries and other financial institutions located in the United States, and Euro clearing through Financial Institution 4 subsidiaries and other financial institutions located in Eurozone countries. A subsidiary of Financial Institution 4 ("U.S. Subsidiary 4"), an entity whose identity is known to the Grand Jury, was a financial institution organized in the United States offering banking and financial services throughout the world. U.S. Subsidiary 4 offered HUAWEI and its affiliates banking services and cash management services, including for accounts in the United States.
III. The SKYCOM Fraud Scheme

11. Even though the U.S. Department of the Treasury’s Office of Foreign Assets Control’s (“OFAC”) Iranian Transactions and Sanctions Regulations (“ITSR”), 31 C.F.R. Part 560, proscribed the export of U.S.-origin goods, technology and services to Iran and the Government of Iran, HUAWEI operated SKYCOM as an unofficial subsidiary to obtain otherwise prohibited U.S.-origin goods, technology and services, including banking services, for HUAWEI’s Iran-based business while concealing the link to HUAWEI. HUAWEI could thus attempt to claim ignorance with respect to any illegal act committed by SKYCOM on behalf of HUAWEI, including violations of the ITSR and other applicable U.S. law. In addition, contrary to U.S. law, SKYCOM, on behalf of HUAWEI, employed in Iran at least one U.S. citizen (“Employee 1”), whose identity is known to the Grand Jury.

12. Since in or about July 2007, HUAWEI repeatedly misrepresented to the U.S. government and to various victim financial institutions, including Financial Institutions 1, 2, 3 and 4, and their U.S. and Eurozone subsidiaries and branches (collectively, the “Victim Institutions”), that, although HUAWEI conducted business in Iran, it did so in a manner that did not violate applicable U.S. law, including the ITSR. In reality, HUAWEI conducted its business in Iran in a manner that violated applicable U.S. law, which includes the ITSR.

13. For example, in or about July 2007, agents with the Federal Bureau of Investigation (“FBI”) interviewed the founder of HUAWEI (“Individual-1”), whose identity is known to the Grand Jury, in New York, New York. Individual-1 stated, in sum and substance, that he was willing to provide information about HUAWEI.
14. During the interview, amongst other things, Individual-1 falsely stated, in substance and in part, that HUAWEI did not conduct any activity in violation of U.S. export laws and that HUAWEI operated in compliance with all U.S. export laws. Individual-1 also falsely stated, in substance and in part, that HUAWEI had not dealt directly with any Iranian company. Individual-1 further stated that he believed HUAWEI had sold equipment to a third party, possibly in Egypt, which in turn sold the equipment to Iran.

15. Additionally, HUAWEI repeatedly misrepresented to Financial Institution 1 that HUAWEI would not use Financial Institution 1 and its affiliates to process any transactions regarding HUAWEI’s Iran-based business. In reality, HUAWEI used U.S. Subsidiary 1 and other financial institutions operating in the United States to process U.S.-dollar clearing transactions involving millions of dollars in furtherance of HUAWEI’s Iran-based business. Some of these transactions passed through the Eastern District of New York.

16. In or about late 2012 and early 2013, various news organizations, including Reuters, reported that SKYCOM had sold and attempted to sell embargoed U.S.-origin goods to Iran in violation of U.S. law, and that HUAWEI in fact owned and operated SKYCOM. In December 2012, Reuters published an article purporting to contain a HUAWEI official statement addressing and denying those allegations. In January 2013, Reuters published a second article purporting to contain a HUAWEI official statement, again addressing and denying the Iran allegations. The purported statements by HUAWEI in these articles were relied on by the Victim Institutions in determining whether to continue their banking relationships with HUAWEI and its subsidiaries.
17. Following publication of the December 2012 and January 2013 Reuters articles, various HUAWEI representatives and employees communicated to the Victim Institutions and to the public that the allegations regarding HUAWEI's ownership and control of SKYCOM were false and that, in fact, HUAWEI did comply with applicable U.S. law, which includes the ITSR. Based in part on these false representations, the Victim Institutions continued their banking relationships with HUAWEI and its subsidiaries and affiliates.

18. For example, in or about June 2013, the defendant WANZHOU MENG requested an in-person meeting with a Financial Institution 1 executive (the "Financial Institution 1 Executive"), whose identity is known to the Grand Jury. During the meeting, which took place on or about August 22, 2013, MENG spoke in Chinese, relying in part on a PowerPoint presentation written in Chinese. Upon request by the Financial Institution 1 Executive, MENG arranged for an English-language version of the PowerPoint presentation to be delivered to Financial Institution 1 on or about September 3, 2013.

19. In relevant part, the PowerPoint presentation included numerous misrepresentations regarding HUAWEI's ownership and control of SKYCOM and HUAWEI's compliance with applicable U.S. law, including that (1) HUAWEI "operates in Iran in strict compliance with applicable laws, regulations and sanctions of UN, US and EU"; (2) "HUAWEI’s engagement with SKYCOM is normal business cooperation"; (3) the defendant WANZHOU MENG’s participation on the Board of Directors of SKYCOM was to "help HUAWEI to better understand SKYCOM’s financial results and business performance, and to strengthen and monitor SKYCOM’s compliance"; and (4) "HUAWEI
subsidiaries in sensitive countries will not open accounts at [Financial Institution 1], nor have business transactions with [Financial Institution 1].” These statements were all false.

20. In early 2014, several months after the meeting with Financial Institution 1 Executive, the defendant WANZHOU MENG traveled to the United States, arriving at John F. Kennedy International Airport, which is located in the Eastern District of New York. When she entered the United States, MENG was carrying an electronic device that contained a file in unallocated space—indicating that the file may have been deleted—containing the following text:

Suggested Talking Points

The core of the suggested talking points regarding Iran/Skycom: Huawei’s operation in Iran comports with the laws, regulations and sanctions as required by the United Nations, the United States and the European Union. The relationship with Skycom is that of normal business cooperation. Through regulated trade organizations and procedures, Huawei requires that Skycom promises to abide by relevant laws and regulations and export controls. Key information 1: In the past — ceased to hold Skycom shares 1, With regards to cooperation: Skycom was established in 1998 and is one of the agents for Huawei products and services. Skycom is mainly an agent for Huawei.

Other text in the same file appeared to refer to a document announcing the appointment of Huawei employees that was “signed by MENG Wanzhou,” the defendant.

21. Based in part on the false representations made by the defendant WANZHOU MENG and others, Financial Institution 1 continued its banking relationship with HUAWEI and its subsidiaries and affiliates.

22. Had the Victim Institutions known about HUAWEI’s repeated violations of the ITSR, they would have reevaluated their banking relationships with HUAWEI, including the provision of U.S.-dollar and Euro clearing services to HUAWEI.
IV. HUAWEI's Continued Scheme to Defraud Financial Institutions

23. In or about 2017, Financial Institution 1 decided to terminate its global relationship with HUAWEI because of risk concerns regarding HUAWEI's business practices. During a series of meetings and communications, Financial Institution 1 repeatedly communicated to HUAWEI that the decision to terminate its banking relationship with HUAWEI had been made by Financial Institution 1 alone, and was not a mutual decision with HUAWEI.

24. After learning of Financial Institution 1's decision to terminate its relationship with HUAWEI, HUAWEI took steps to secure and expand its banking relationships with other financial institutions, including U.S. Subsidiary 4. In doing so, HUAWEI employees made material misrepresentations to U.S. Subsidiary 4, among other financial institutions, regarding the reason for the termination of its relationship with Financial Institution 1 and the party responsible for the termination, claiming that HUAWEI, not Financial Institution 1, had initiated the termination. Specifically, in meetings and correspondence with representatives of U.S. Subsidiary 4, HUAWEI employees falsely represented that HUAWEI was considering terminating its relationship with Financial Institution 1 because HUAWEI was dissatisfied with Financial Institution 1's level of service. HUAWEI's misrepresentation that it had decided to terminate its relationship with Financial Institution 1 was communicated to various components of U.S. Subsidiary 4, including in New York City.

25. Based in part on these false representations and omissions made by the defendants HUAWEI, among other HUAWEI employees, U.S. Subsidiary 4 undertook to expand its banking relationship with HUAWEI
and its subsidiaries and affiliates, and continued to maintain its existing banking relationship with HUAWEI globally, including in the United States. Had the defendants told U.S. Subsidiary 4 the truth about Financial Institution 1’s decision to terminate its relationship with HUAWEI, U.S. Subsidiary 4 would have reevaluated its relationship with HUAWEI and its subsidiaries and affiliates.

V. The Scheme to Obstruct Justice

26. In or about 2017, HUAWEI and HUAWEI USA became aware of the U.S. government’s criminal investigation of HUAWEI and its affiliates. In response to the investigation, HUAWEI and HUAWEI USA made efforts to move witnesses with knowledge about HUAWEI’s Iran-based business to the PRC, and beyond the jurisdiction of the U.S. government, and to destroy and conceal evidence in the United States of HUAWEI’s Iran-based business.

COUNT ONE
(Conspiracy to Commit Bank Fraud)

27. The allegations contained in paragraphs one through 22 are realleged and incorporated as if set forth fully in this paragraph.

28. In or about and between November 2007 and May 2015, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants HUAWEI, SKYCOM and WANZHOU MENG, also known as “Cathy Meng” and “Sabrina Meng,” together with others, did knowingly and intentionally conspire to execute a scheme and artifice to defraud U.S. Subsidiary 1, a financial institution, and to obtain moneys, funds, credits and other property owned by and under the custody and control of said financial institution, by means of one or more materially false and fraudulent
pretenses, representations and promises, contrary to Title 18, United States Code, Section 1344.

(Title 18, United States Code, Sections 1349 and 3551 et seq.)

COUNT TWO
(Conspiracy to Commit Bank Fraud)

29. The allegations contained in paragraphs one through 25 are realleged and incorporated as if set forth fully in this paragraph.

30. In or about and between August 2017 and the date of the filing of this Superseding Indictment, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants HUAWEI, [redacted] together with others, did knowingly and intentionally conspire to execute a scheme and artifice to defraud U.S. Subsidiary 4, a financial institution, and to obtain moneys, funds, credits and other property owned by and under the custody and control of said financial institution, by means of one or more materially false and fraudulent pretenses, representations and promises, contrary to Title 18, United States Code, Section 1344.

(Title 18, United States Code, Sections 1349 and 3551 et seq.)

COUNT THREE
(Conspiracy to Commit Wire Fraud)

31. The allegations contained in paragraphs one through 22 are realleged and incorporated as if set forth fully in this paragraph.

32. In or about and between November 2007 and May 2015, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants HUAWEI, SKYCOM and WANZhou MENG, also known as “Cathy Meng”
and “Sabrina Meng,” together with others, did knowingly and intentionally conspire to devise a scheme and artifice to defraud the Victim Institutions, and to obtain money and property from the Victim Institutions, by means of one or more materially false and fraudulent pretenses, representations and promises, and for the purpose of executing such scheme and artifice, to transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures and sounds, contrary to Title 18, United States Code, Section 1343.

(Title 18, United States Code, Sections 1349 and 3551 et seq.)

COUNT FOUR
(Bank Fraud)

33. The allegations contained in paragraphs one through 22 are realleged and incorporated as if set forth fully in this paragraph.

34. In or about and between November 2007 and May 2015, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants HUAWEI, SKYCOM and WANZHOU MENG, also known as “Cathy Meng” and “Sabrina Meng,” together with others, did knowingly and intentionally execute a scheme and artifice to defraud U.S. Subsidiary 1, a financial institution, and to obtain moneys, funds, credits and other property owned by, and under the custody and control of said financial institution, by means of one or more materially false and fraudulent pretenses, representations and promises.

(Title 18, United States Code, Sections 1344, 2 and 3551 et seq.)
COUNT FIVE
(Bank Fraud)

35. The allegations contained in paragraphs one through 25 are realleged and incorporated as if set forth fully in this paragraph.

36. In or about and between August 2017 and the date of the filing of this Superseding Indictment, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants HUAWEI, together with others, did knowingly and intentionally execute a scheme and artifice to defraud U.S. Subsidiary 4, a financial institution, and to obtain moneys, funds, credits and other property owned by, and under the custody and control of said financial institution, by means of one or more materially false and fraudulent pretenses, representations and promises.

(Title 18, United States Code, Sections 1344, 2 and 3551 et seq.)

COUNT SIX
(Wire Fraud)

37. The allegations contained in paragraphs one through 22 are realleged and incorporated as if set forth fully in this paragraph.

38. In or about and between November 2007 and May 2015, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants HUAWEI, SKYCOM and WANZHOUMENG, also known as “Cathy Meng” and “Sabrina Meng,” together with others, did knowingly and intentionally devise a scheme and artifice to defraud the Victim Institutions, and to obtain money and property from the Victim Institutions, by means of one or more materially false and fraudulent pretenses, representations and promises, and for the purpose of executing such scheme and artifice, did
transmit and cause to be transmitted by means of wire communication in interstate and
foreign commerce, writings, signs, signals, pictures and sounds, to wit: the defendants
HUAWEI, SKYCOM and MENG, together with others, (a) made, and caused to be made, a
series of misrepresentations through email communications, written communications
otherwise conveyed through the wires, and oral communications made with knowledge that
the oral communications would be memorialized and subsequently transmitted through the
wires, about, among other things, the relationship between HUAWEI and SKYCOM,
HUAWEI’s compliance with U.S. and U.N. laws and regulations, and the kinds of financial
transactions in which HUAWEI engaged through the Victim Institutions; and (b) as a result
of the misrepresentations, caused a series of wires to be sent by financial institutions from
outside of the United States through the United States.

(Title 18, United States Code, Sections 1343, 2 and 3551 et seq.)

COUNT SEVEN
(Conspiracy to Defraud the United States)

39. The allegations contained in paragraphs one through 26 are realleged
and incorporated as if set forth fully in this paragraph.

40. In or about and between July 2007 and the date of the filing of this
Superseding Indictment, both dates being approximate and inclusive, within the Eastern
District of New York and elsewhere, the defendants HUAWEI and SKYCOM, together with
others, did knowingly and willfully conspire to defraud the United States by impairing,
impeding, obstructing and defeating, through deceitful and dishonest means, the lawful
governmental functions and operations of OFAC, an agency of the United States, in the
enforcement of economic sanctions laws and regulations administered by that agency and the
issuance by that agency of appropriate licenses relating to the provision of financial services.

41. In furtherance of the conspiracy and to effect its objects, within the
Eastern District of New York and elsewhere, the defendants HUAWEI and SKYCOM,
together with others, committed and caused to be committed, among others, the following:

OVERT ACTS

a. On or about July 11, 2007, Individual-1 stated to FBI agents that
HUAWEI did not conduct any activity in violation of U.S. export laws, that HUAWEI,
operated in compliance with all U.S. export laws, that HUAWEI had not dealt directly with
any Iranian company and that he believed HUAWEI had sold equipment to a third party,
possibly in Egypt, which in turn sold the equipment to Iran.

b. On or about September 13, 2012, a Senior Vice President of
HUAWEI testified before U.S. Congress that HUAWEI's business in Iran had not “violated
any laws and regulations including sanction-related requirements.”

c. On or about September 17, 2012, the Treasurer of HUAWEI
met with a principal of U.S. Subsidiary 4, an individual whose identity is known to the Grand
Jury, in New York, New York, and informed U.S. Subsidiary 4 that HUAWEI and its global
affiliates did not violate any applicable U.S. law.

d. On or about July 24, 2013, SKYCOM caused U.S. Subsidiary 1
to process a U.S.-dollar clearing transaction of $52,791.08.

e. On or about July 24, 2013, SKYCOM caused a bank located in
the Eastern District of New York (“Bank 1”), an entity whose identity is known to the Grand
Jury, to process a U.S.-dollar clearing transaction of $94,829.82.
f. On or about August 20, 2013, SKYCOM caused Bank 1 to process a U.S.-dollar clearing transaction of $14,835.22.

g. On or about August 28, 2013, SKYCOM caused Bank 1 to process a U.S.-dollar clearing transaction of $32,663.10.

h. On or about April 11, 2014, SKYCOM caused a bank located in the United States ("Bank 2"), an entity whose identity is known to the Grand Jury, to process a U.S.-dollar clearing transaction of $118,842.45.

(Title 18, United States Code, Sections 371 and 3551 et seq.)

COUNT EIGHT
(Conspiracy to Violate IEEPA)

42. The allegations contained in paragraphs one through 22 are realleged and incorporated as if set forth fully in this paragraph.

43. Through the International Emergency Economic Powers Act ("IEEPA"), the President of the United States was granted authority to address unusual and extraordinary threats to the national security, foreign policy or economy of the United States. 50 U.S.C. § 1701(a). Under IEEPA, it was a crime to willfully violate, attempt to violate, conspire to violate or cause a violation of any license, order, regulation or prohibition issued pursuant to the statute. 50 U.S.C. §§ 1705(a) and 1705(c).

44. To respond to the declaration by the President of a national emergency with respect to Iran pursuant to IEEPA, which was most recently continued in March 2018 (83 Fed. Reg. 11,393 (Mar. 14, 2018)), OFAC issued the ITSR. Absent permission from OFAC in the form of a license, these regulations prohibited, among other things:
a. The exportation, reexportation, sale or supply from the United States, or by a U.S. person, wherever located, of any goods, technology or services to Iran and the Government of Iran (31 C.F.R. § 560.204);

b. Any transaction by a U.S. person, wherever located, involving goods, technology or services for exportation, reexportation, sale or supply, directly or indirectly, to Iran or the Government of Iran (31 C.F.R. § 560.206); and

c. Any transaction by a U.S. person, or within the United States, that evaded or avoided, had the purpose of evading or avoiding, attempted to violate, or caused a violation of any of the prohibitions in the ITSR (31 C.F.R. § 560.203).

45. The ITSR prohibited providing financial services, including U.S. dollar-clearing services, to Iran or the Government of Iran. 31 C.F.R. §§ 560.204, 560.427. In addition, the prohibition against the exportation, reexportation, sale or supply of services applied to services performed on behalf of a person in Iran or the Government of Iran, or where the benefit of such services was otherwise received in Iran, if the services were performed (a) in the United States by any person; or (b) outside the United States by a United States person, including an overseas branch of an entity located in the United States. 31 C.F.R. § 560.410.

46. In or about and between November 2007 and November 2014, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants HUAWEI and SKYCOM, together with others, did knowingly and willfully conspire to cause the export, reexport, sale and supply, directly and indirectly, of goods, technology and services, to wit: banking and other financial services from the United States to Iran and the Government of Iran, without having first obtained the required OFAC
license, contrary to Title 31, Code of Federal Regulations, Sections 560.203, 560.204 and 560.206.

(Title 50, United States Code, Sections 1705(a), 1705(c) and 1702; Title 18, United States Code, Sections 3551 et seq.)

COUNT NINE
(IEEPA Violations)

47. The allegations contained in paragraphs one through 22 and 43 through 45 are realleged and incorporated as if fully set forth in this paragraph.

48. In or about and between November 2007 and November 2014, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants HUAWEI and SKYCOM, together with others, did knowingly and willfully cause the export, reexport, sale and supply, directly and indirectly, of goods, technology and services, to wit: banking and other financial services from the United States to Iran and the Government of Iran, without having first obtained the required OFAC license, contrary to Title 31, Code of Federal Regulations, Sections 560.203, 560.204 and 560.206.

(Title 50, United States Code, Sections 1705(a), 1705(c) and 1702; Title 18, United States Code, Sections 2 and 3551 et seq.)

COUNT TEN
(Conspiracy to Violate IEEPA)

49. The allegations contained in paragraphs one through 22 and 43 through 45 are realleged and incorporated as if fully set forth in this paragraph.

50. In or about and between 2008 and 2014, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants
HUAWEI and SKYCOM, together with others, did knowingly and willfully conspire to cause the export, reexport, sale and supply, directly and indirectly, of goods, technology and services, to wit: telecommunications services provided by Employee 1, a U.S. citizen, to Iran and the Government of Iran, without having first obtained the required OFAC license, contrary to Title 31, Code of Federal Regulations, Sections 560.203, 560.204 and 560.206.

(Title 50, United States Code, Sections 1705(a), 1705(c) and 1702; Title 18, United States Code, Sections 3551 et seq.)

COUNT ELEVEN
(IEEPA Violation)

51. The allegations contained in paragraphs one through 22 and 43 through 45 are realleged and incorporated as if fully set forth in this paragraph.

52. In or about and between 2008 and 2014, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants HUAWEI and SKYCOM, together with others, did knowingly and willfully cause the export, reexport, sale and supply, directly and indirectly, of goods, technology and services, to wit: telecommunications services provided by Employee 1, a U.S. citizen, to Iran and the Government of Iran, without having first obtained the required OFAC license, contrary to Title 31, Code of Federal Regulations, Sections 560.203, 560.204 and 560.206.

(Title 50, United States Code, Sections 1705(a), 1705(c) and 1702; Title 18, United States Code, Sections 2 and 3551 et seq.)

COUNT TWELVE
(Money Laundering Conspiracy)

53. The allegations contained in paragraphs one through 22 and 43 through 45 are realleged and incorporated as if fully set forth in this paragraph.
54. In or about and between November 2007 and November 2014, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants HUAWEI and SKYCOM, together with others, did knowingly and intentionally conspire to transport, transmit and transfer monetary instruments and funds, to wit: wire transfers, from one or more places in the United States to and through one or more places outside the United States and to one or more places in the United States from and through one or more places outside the United States, with the intent to promote the carrying on of specified unlawful activity, to wit: conspiracy to violate IEEPA, in violation of Title 50, United States Code, Section 1705, all contrary to Title 18, United States Code, Section 1956(a)(2)(A).

(Title 18, United States Code, Sections 1956(h) and 3551 et seq.)

COUNT THIRTEEN
(Conspiracy to Obstruct Justice)

55. The allegations contained in paragraphs one through 22 and 26 are realleged and incorporated as if fully set forth in this paragraph.

56. In or about and between January 2017 and the date of the filing of this Superseding Indictment, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants HUAWEI and HUAWEI USA, together with others, did knowingly, intentionally and corruptly conspire to obstruct, influence and impede an official proceeding, to wit: a Federal Grand Jury investigation in the Eastern District of New York, contrary to Title 18, United States Code, Section 1512(c)(2).

(Title 18, United States Code, Sections 1512(k) and 3551 et seq.)
CRIMINAL FORFEITURE ALLEGATION
AS TO COUNTS ONE THROUGH SIX

57. The United States hereby gives notice to the defendants charged in Counts One through Six that, upon their conviction of such offenses, the government will seek forfeiture in accordance with Title 18, United States Code, Section 982(a)(2), which requires any person convicted of such offenses to forfeit any property constituting, or derived from, proceeds obtained directly or indirectly as a result of such offenses.

58. If any of the above-described forfeitable property, as a result of any act or omission of the defendants:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b)(1), to seek forfeiture of any other property of the defendants up to the value of the forfeitable property described in this forfeiture allegation.

(Title 18, United States Code, Sections 982(a)(2) and 982(b)(1); Title 21, United States Code, Section 853(p))
CRIMINAL FORFEITURE ALLEGATION
AS TO COUNTS EIGHT THROUGH ELEVEN AND THIRTEEN

59. The United States hereby gives notice to the defendants charged in Counts Eight through Eleven and Thirteen that, upon their conviction of such offenses, the government will seek forfeiture in accordance with Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), which require any person convicted of such offenses to forfeit any property, real or personal, constituting, or derived from, proceeds obtained directly or indirectly as a result of such offenses.

60. If any of the above-described forfeitable property, as a result of any act or omission of the defendants:
   a. cannot be located upon the exercise of due diligence;
   b. has been transferred or sold to, or deposited with, a third party;
   c. has been placed beyond the jurisdiction of the court;
   d. has been substantially diminished in value; or
   e. has been commingled with other property which cannot be divided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), to seek forfeiture of any other property of the defendants up to the value of the forfeitable property described in this forfeiture allegation.

(Title 18, United States Code, Section 981(a)(1)(C); Title 21, United States Code, Section 853(p); Title 28, United States Code, Section 2461(c))
CRIMINAL FORFEITURE ALLEGATION
AS TO COUNT TWELVE

61. The United States hereby gives notice to the defendants charged in
Count Twelve that, upon their conviction of such offense, the government will seek
forfeiture in accordance with Title 18, United States Code, Section 982(a)(1), which requires
any person convicted of such offense to forfeit any property, real or personal, involved in
such offense, or any property traceable to such property.

62. If any of the above-described forfeitable property, as a result of any act
or omission of the defendants:

a. cannot be located upon the exercise of due diligence;
b. has been transferred or sold to, or deposited with, a third party;
c. has been placed beyond the jurisdiction of the court;
d. has been substantially diminished in value; or
e. has been commingled with other property which cannot be
   divided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p),
as incorporated by Title 18, United States Code, Section 982(b)(1), to seek forfeiture of any
other property of the defendants up to the value of the forfeitable property described in this
forfeiture allegation.

(Title 18, United States Code, Sections 982(a)(1) and 982(b)(1); Title 21,
United States Code, Section 853(p))

A TRUE BILL

[Signature]
FOREPERSON

RICHARD P. DONOGHUE
UNITED STATES ATTORNEY
EASTERN DISTRICT OF NEW YORK

DEBORAH L. CONNOR
CHIEF
MONEY LAUNDERING
AND ASSET RECOVERY SECTION
CRIMINAL DIVISION
U.S. DEPARTMENT OF JUSTICE

JAY I. BRATT
CHIEF
COUNTERINTELLIGENCE AND EXPORT CONTROL SECTION
NATIONAL SECURITY DIVISION
U.S. DEPARTMENT OF JUSTICE
No.
UNITED STATES DISTRICT COURT
EASTERN District of NEW YORK
CRIMINAL DIVISION

THE UNITED STATES OF AMERICA

vs.

HUawei TECHNOLOGIES CO., LTD., HUAWEI DEvICE USA
INC., SKYCOM TECH CO. LTD., WANZHOU MENG, also known
as "Cathy Meng" and "Sabrina Meng,"

Defendants.

SUPERSEADING INDICTMENT
(T. 18, U.S.C., §§ 371, 981(a)(1)(C); 982(a)(1), 982(a)(2),
982(b)(1)1343, 1344, 1349, 1512(k), 1956(h), 2 and 3551
et seq.; T. 21, U.S.C., § 853(p); T. 28, U.S.C., § 2461(c);
T. 50, U.S.C., §§ 1702, 1705(a) and 1705(c))

A true bill.

Filed in open court this _____ day of _____ A.D. 20____

Clerk

Bail, $ _____

Alexander A. Solomon, David K. Kessler, Julia Nestor, and Sarah
Evans, Assistant U.S. Attorneys (718) 254-7000
UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,
Plaintiff,

v.
HUAWEI DEVICE CO., LTD., and HUAWEI DEVICE USA, INC.,
Defendants.

The Grand Jury charges that:

COUNT 1
(Theft of Trade Secrets Conspiracy)

1. Beginning at a time unknown, but no later than in or about June 2012, and continuing until on or about September 2, 2014, at Bellevue, within the Western District of Washington, and elsewhere, HUAWEI DEVICE CO., LTD., HUAWEI DEVICE USA, INC., and others known and unknown, conspired and agreed together to:

(a) knowingly and without authorization steal, appropriate, take, carry away, and conceal trade secrets belonging to T-Mobile; and by fraud, artifice, and deception obtain trade secrets belonging to T-Mobile;

(b) knowingly and without authorization copy, duplicate, sketch, draw, photograph, download, replicate, transmit, deliver, send, communicate, and convey trade secrets belonging to T-Mobile; and
(c) knowingly receive, buy, and possess trade secrets belonging to T-Mobile, knowing the same to have been stolen, appropriated, obtained, and converted without authorization;

intending to convert a trade secret that is related to a product used and intended for use in interstate and foreign commerce, to the economic benefit of someone other than T-Mobile, and knowing that the offense would injure T-Mobile.

At all times relevant to this Indictment:

A. T-Mobile and the Tappy Robot System.

2. T-Mobile USA, Inc. ("T-Mobile" or "TMO") is one of the largest providers of wireless service in the United States. T-Mobile is headquartered in Bellevue, Washington, and is partially owned by Deutsche Telekom, a German company.

T-Mobile, as part of its business, sells mobile phones that are packaged with wireless service. Although T-Mobile provides the wireless service, third parties manufacture the phones that T-Mobile sells.

3. In or about 2006, T-Mobile began developing a proprietary robotic phone testing system, nicknamed "Tappy." Testing new phones before they are launched is important to wireless carriers such as T-Mobile. This testing identifies software errors and other problems in new phones before they are sold to customers. Correcting these errors prior to launching a new phone helps enable T-Mobile and other carriers to avoid damaging their reputation by launching phones in the market that suffer from software bugs or other problems, and to avoid the significant costs associated with customer returns of defective devices.

4. T-Mobile created Tappy to be an innovative way to test phones. T-Mobile developed and refined the Tappy system over several years, at significant expense to T-Mobile, both in terms of actual dollars expended and employee time to develop and refine the system. The Tappy robot is a largely automated testing process that tests a phone for an extended period to measure the phone's performance and stability under prolonged usage, saving the employee time that would be expended with manual testing.
of the phone. The Tappy robot performs “touches” on phones that simulate how people use their phones. Tappy tests, among other things, the responsiveness, performance, and stability of the phone’s user interface. Tappy also records and tracks the phone’s performance during testing, including measuring the battery life expended by particular tasks. Tappy’s largely automated testing system was unique as compared to the way other wireless carriers tested phones at the time, which typically involved software that performed a variety of tests on phones or manually testing phones to approximate how customers would use them.

5. Tappy was valuable to T-Mobile for several reasons. First, T-Mobile found that Tappy was an improvement over other testing systems in the market. This improvement was reflected in the fact that T-Mobile experienced a significant decline in customer returns after Tappy was implemented, which reduced costs for T-Mobile. Tappy played a part in this decline by catching errors and problems upfront before T-Mobile released the phones in the market. Second, T-Mobile believed that Tappy provided the company with a competitive edge over other wireless carriers, none of which used a robotic testing system. T-Mobile publicly marketed Tappy as improving phone quality, which contributed to the value of the T-Mobile brand. Third, Tappy had significant potential licensing and sales value for T-Mobile. Over time, T-Mobile received multiple inquiries about licensing or purchasing the Tappy system. As the exclusive owner and holder of this technology, T-Mobile had the option to sell Tappy for a price that would have been higher than if the system were available from other parties as well. In this way, Tappy represented a valuable asset that T-Mobile had the option of further monetizing.

6. In recognition of its proprietary value, T-Mobile implemented a number of measures to protect the Tappy technology and keep it confidential. For example, T-Mobile housed its Tappy robots in a secure laboratory at its headquarters that required special badge access to enter. The laboratory had security cameras and a security guard posted at the front desk of the building that housed the laboratory. T-Mobile patented
Case 2:19-cr-00010-RSM  Document 1  Filed 01/16/19  Page 4 of 28

1 various aspects of Tappy – although the system could not be replicated solely from the
2 patent materials. T-Mobile also kept a secure hold on the details about how Tappy was
3 constructed, and declined the offers described above to license or sell the technology to
4 phone manufacturers and other third parties.
5
6 7. When T-Mobile initially implemented Tappy, only T-Mobile employees
7 were allowed to operate the robot. Over time, T-Mobile allowed approved employees
8 from phone suppliers to use Tappy to test phones that were scheduled for release. With
9 this expanded access, T-Mobile implemented a series of additional measures to safeguard
10 the confidentiality of Tappy and its technology. For example, T-Mobile set up a separate
11 portion of its laboratory for suppliers to test phones on Tappy. T-Mobile also required
12 suppliers to execute nondisclosure and confidentiality agreements before being able to
13 access and operate Tappy. These agreements included multiple confidentiality
14 provisions, including provisions barring suppliers’ employees from attempting to reverse
15 engineer Tappy, or take any photographs or videos of the Tappy robots. T-Mobile
16 limited access to Tappy to only a select few employees from each supplier; these
17 suppliers’ employees were approved and trained by T-Mobile. Moreover, T-Mobile
18 permitted these employees to access Tappy only from within T-Mobile’s secure
19 laboratory, only for limited time periods, and only to test phones that were scheduled for
20 release and for no other purpose.

21 B. T-Mobile’s Business Relationship with Huawei.

22 8. Huawei is a telecommunications company that, among other things,
23 manufactures and sells phones to wireless carriers. Huawei operates through multiple
24 corporate entities, including as HUAWEI DEVICE CO., LTD. (“HUAWEI CHINA”),
25 which is located in China, and HUAWEI DEVICE USA, INC. (“HUAWEI USA”),
26 which operates in the United States, with offices in Bellevue, Washington, and Plano,
27 Texas, among other locations. HUAWEI CHINA designs and manufactures wireless
28 phones. HUAWEI USA sells and distributes Huawei products, including wireless

 carriers and facilitating the resolution of issues reported during testing with HUAWEI
CHINA.

9. In June 2010, Futurewei Technologies, Inc. d/b/a Huawei Technologies
(USA), the predecessor corporation of HUAWEI USA, entered into a Supply Agreement
with T-Mobile to supply wireless phones to T-Mobile. The terms of this Supply
Agreement made it binding upon any successor entities, such as HUAWEI USA. Under
this Supply Agreement, HUAWEI USA’s predecessor acknowledged that it would be
receiving confidential information from T-Mobile as part of their business relationship,
including trade secrets, intellectual property, and technical information. HUAWEI USA’s
predecessor agreed that such confidential information would remain T-Mobile’s
exclusive property and that it would not use such information except in the performance
of its agreement with T-Mobile.

10. In 2011, pursuant to this Supply Agreement, Huawei began supplying
phones to T-Mobile that T-Mobile subsequently marketed and sold throughout the United
States. Prior to this time, Huawei had no measurable share of the wireless phone market
in the United States, the third largest wireless phone market in the world. Huawei placed
great value on developing its relationship with T-Mobile, and viewed that relationship as
an important step to gaining a foothold in the United States market.

11. In or about August 2012, T-Mobile agreed to grant HUAWEI USA
engineers access to T-Mobile’s Tappy robotic testing system for the purpose of testing
Huawei phones prior to their release. Prior to granting this access, T-Mobile required
HUAWEI USA to execute two nondisclosure agreements containing multiple
confidentiality provisions. HUAWEI USA, with the knowledge and approval of
HUAWEI CHINA, executed these two nondisclosure agreements on August 14, 2012,
and August 16, 2012. Under the terms of the agreements, HUAWEI USA executed them
“on behalf of itself, its parents, [and] affiliates,” including HUAWEI CHINA. In these
agreements, HUAWEI USA made material promises and representations to T-Mobile,
including that its employees would not, among other things: (a) photograph T-Mobile’s
Tappy robotic testing system; (b) attempt to copy or discover Tappy’s software source
codes or trade secrets; (c) attempt to reverse-engineer Tappy’s software or hardware
components; or (d) attempt to circumvent any security measures that prevented
unauthorized access to Tappy. In addition, HUAWEI USA represented in the
nondisclosure agreements that its employees would access the Tappy system solely for
the purpose of testing Huawei phones, and for no other purpose, and that it would not use
T-Mobile’s confidential information except in the performance of its agreement with
T-Mobile. T-Mobile relied upon all of the representations made by HUAWEI USA in
the nondisclosure agreements in granting HUAWEI USA’s employees access to Tappy.
In mid-September 2012, based on the representations made by HUAWEI USA in these
agreements, T-Mobile began to admit approved HUAWEI USA employees to the Tappy
robot laboratory for phone testing.

C. Huawei’s Efforts to Steal Tappy’s Technology.

12. During in or about 2012, HUAWEI CHINA began developing its own
phone testing robot, known as xDeviceRobot. HUAWEI CHINA intended to use
xDeviceRobot in China to test the phones it would supply to T-Mobile and other
competing wireless carriers, including China Mobile and AT&T. HUAWEI CHINA was
attempting to design its own robotic testing system for multiple reasons. First, the phones
that HUAWEI CHINA supplied to T-Mobile generally were not of high quality, and the
phones were failing Tappy’s testing at a disproportionate rate compared to other
suppliers’ phones. HUAWEI CHINA hoped that it could improve the quality of phones
that it supplied to T-Mobile by utilizing its own robot testing earlier in the process, while
the phones were still under development in China. Second, HUAWEI CHINA hoped that
robotic testing would improve the quality of its phones generally, including phones that it
supplied to competing wireless carriers, including China Mobile and AT&T.

13. In early May 2012, while the above-referenced nondisclosure agreements
were being drafted and negotiated, R.Y., the HUAWEI USA Director of Technical
Acceptance, inquired, on behalf of HUAWEI CHINA, whether T-Mobile would be
willing to sell or license the Tappy robot system to HUAWEI CHINA. T-Mobile
declined to do so. R.Y. then communicated to engineers at HUAWEI CHINA that
T-Mobile had “no plan to sell the robot system” to phone manufacturers such as Huawei.
He further explained that T-Mobile’s reasons for this included that it did not want the
Tappy technology to be used to improve phones that Huawei would supply to T-Mobile’s
competitors, such as AT&T, and it did not want to reveal Tappy’s software source code
to phone manufacturers such as Huawei.

14. After that, in 2012 and continuing through May 2013, HUAWEI CHINA,
with help from HUAWEI USA employees, undertook a scheme to steal T-Mobile’s
Tappy technology for use in the development of its xDeviceRobot. In furtherance of this
scheme, and over the course of numerous telephonic and electronic communications,
HUAWEI CHINA employees who were involved in the development of the
xDeviceRobot directed HUAWEI USA employees who had access to Tappy to gather a
variety of technical details about Tappy.

15. On or about June 30, 2012, F.W., a HUAWEI CHINA engineer working on
the xDeviceRobot project, convened a conference call with multiple HUAWEI USA and
HUAWEI CHINA engineers. F.W. created a list of questions for HUAWEI USA
employees to answer about the Tappy robot, including requesting photos of the Tappy
robot from different angles, and detailed technical specifications of Tappy, including
component serial numbers, camera resolution, the sliding speed of the mechanical arm,
and the method of calculating the user interface response time. HUAWEI USA engineer
H.L., in turn, posed many of these same questions to T-Mobile engineers. In response to
these and similar questions, T-Mobile employees provided only limited information
about Tappy and declined to provide additional information about the technical
specifications of the Tappy system. H.L. and other HUAWEI USA employees informed
the HUAWEI CHINA engineers that T-Mobile was unwilling to provide this sort of
information due to “information security regulations.”
16. During August and September 2012, by email and other communications, HUAWEI CHINA engineers continued to task HUAWEI USA employees with determining the technical specifications of the Tappy robot, despite having been made aware that T-Mobile was unwilling to disclose confidential technical information about Tappy. For example, in an email sent on September 10, 2012, H.P., HUAWEI CHINA’s Director of Device Testing Management Department, stated, “The main point is to figure out the [Tappy] Robot’s specifications and functions. These are the benchmarks of products developed by ourselves.” HUAWEI USA employee R.Y. replied that T-Mobile was unwilling to provide this sort of technical information. In emails sent on September 8 and 11, 2012, R.Y. explained that T-Mobile was unwilling “to share the detail of robot tech/docs” with suppliers, such as Huawei, and that T-Mobile refused to “provide us the details of robot hardware and software specifications.”

17. On November 6, 2012, HUAWEI CHINA engineer J.Y. sent an email to HUAWEI USA employee R.Y. stating: “[T]his email is just a kindly reminder for the information we need to build our own robot system and kindly feedback the information we need in the attachment. . .” Attached to the email was a PowerPoint file requesting information about the technical specifications of the Tappy robot hardware components and software systems. On November 7, 2012, R.Y. forwarded this email to two HUAWEI USA engineers, including A.X., and directed them to provide the requested information to HUAWEI CHINA. R.Y. also assured J.Y.: “[The HUAWEI USA engineers] have accessed the [T-Mobile] robot lab . . . They know how TMO robot work and system info. I asked them to write down the info in detail and then send to [HUAWEI CHINA].”

18. On November 15, 2012, HUAWEI USA engineer A.X. replied to J.Y.: “I am sorry we can not get more information from TMO and we can’t finish the whole [PowerPoint] as we talk about. And as you know, we can take some pictures of test procedure and setting. Hope it is useful to HQ R&D.” The following day, on November 16, 2012, A.X. sent an email to J.Y. and other HUAWEI CHINA engineers with multiple
unauthorized photos of the Tappy robot and its software interface system that A.X. had
taken inside of the secure T-Mobile lab, in violation of the nondisclosure agreements
HUAWEI USA signed.

19. In December 2012, HUAWEI CHINA engineers continued to task the
HUAWEI USA employees to provide them with the same technical specifications and
details about Tappy that T-Mobile previously had declined to share with HUAWEI USA
and HUAWEI CHINA. T-Mobile again refused to provide this information. On
December 20, 2012, R.Y. informed J.Y. and other HUAWEI CHINA engineers: “We got
not much information from TMO on these questions that you guys asked. Again, TMO
won’t want to share any more information about their robot system with us. However,
we still try to find more information during our test in TMO robot lab. But it won’t
expect anytime soon.”

20. On December 31, 2012, J.Y. sent an email to multiple HUAWEI CHINA
engineers and HUAWEI USA employees, including R.Y. and A.X., stating: “We are still
working on the Robot system and we had some issues with the system at the moment.”
J.Y. then asked the HUAWEI USA employees detailed information about Tappy,
including whether the software test scripts were customized per device, about the touch
speed of the robot system, about how the rubber tip was installed on the robot system,
and whether there was any air space inside of the tip. On January 1, 2013, A.X. replied
with answers to some of these questions, and attached unauthorized photographs of the
Tappy robot system that he had taken inside of the secure T-Mobile lab, in violation of
the nondisclosure agreements HUAWEI USA signed.

21. On January 5, 2013, J.Y. sent another email to HUAWEI USA employees,
including R.Y. and A.X., asking them for additional technical information about the
Tappy robot system, specifically seeking details about “the response time accuracy of
TMO’s mechanical arm.” That same day, A.X. replied that T-Mobile would not provide
that information. On January 7, 2013, R.Y. sent an email to J.Y. and other
HUAWEI CHINA engineers emphasizing: “Once again, we CAN’T ask TMO any
questions about the robot. TMO is VERY angry the questions that we asked. Sorry we
can't deliver any more information to you.” R.Y. suggested that HUAWEI CHINA send
its own engineer to Seattle to gain direct access to Tappy, stating, “You will learn a lot in
knowledge and experience.”

22. During March and April 2013, HUAWEI CHINA engineers continued to
task HUAWEI USA employees to provide them with the same sorts of technical
specifications and details about Tappy that T-Mobile previously had declined to share.
For example, on or about March 28, 2013, F.W., a HUAWEI CHINA engineer working
on the xDeviceRobot project, sent an email to HUAWEI USA engineer H.L. and other
HUAWEI CHINA and HUAWEI USA employees, stating, “From the results of the
recent xDeviceRobot system [] verification, there is still a definite disparity with
T-Mobile [robot].” F.W. tasked H.L. to obtain and provide information about the Tappy
robot arm and end effector tip, including its contact hardness, contact area, and pressure.
H.L. replied that HUAWEI CHINA should contact the manufacturer of the Tappy robot
arm directly, rather than having HUAWEI USA try to get the requested information from
T-Mobile. H.L. explained that going through T-Mobile “would only backfire” and that
“[a]fter signing a confidentiality agreement at the TMO laboratory, the relevance of this
information to us was very sensitive.”

23. By in or about mid-April 2013, HUAWEI CHINA was encountering
difficulties with its development of the xDeviceRobot, and HUAWEI CHINA engineers
continued to direct HUAWEI USA employees to attempt to steal information about
Tappy. On April 12, 2013, HUAWEI CHINA engineer J.Y. sent an email to several
HUAWEI CHINA employees, including the leader of the xDeviceRobot development
team, and HUAWEI USA employees, including R.Y. and A.X. The email tasked the
HUAWEI USA employees to provide additional technical information about, among
other things, Tappy’s calibration standards and what tools and software Tappy used to
calculate delays during performance testing.
24. On April 12, 2013, in response to the above-referenced email from J.Y., HUAWEI USA employee R.Y. again suggested that HUAWEI CHINA send its own engineer to the United States who could access Tappy directly and thereby surreptitiously learn the information that HUAWEI CHINA was seeking, but that T-Mobile had been refusing to provide. Specifically, R.Y. stated:

First of all, I am glad that HQ R&D has been continuing to improve HUAWEI robot system. Based on the test on [T-Mobile phone] we do see a big difference of test results between TMO robot and Huawei robot. I think we have a lot of work to improve our robot performance. The difference between two is not only the hardware but also (most importantly) the software. TMO has spend much more money on software than hardware.

Once again, we can’t get any further information about TMO robot system from TMO. They have complained [to] us a lot about this because we asked them too many questions of the robot based on HQ’s request. TMO said to me that if we ask them again such questions, they don’t allow us to use their robot Lab. . . . TMO has set up a security system by putting camera into the robot Lab. I think everyone knows what this means. . . . We can’t provide any further information to HQ because we can’t get anything from TMO.

Once again, I suggested HQ to send an engineer to TMO for a hands-on experience by playing the robot system. I believe this would give HQ robot team a huge benefit in understanding TMO robot system from hardware and software, as well as operation.

25. On April 12, 2013, another HUAWEI USA employee, who served as a manager in the Technical Acceptance Department, replied to the above email string and explained his understanding of the reasons why T-Mobile considered the Tappy robot to be confidential and proprietary property, and was refusing to provide HUAWEI USA and HUAWEI CHINA with the technical specifications and details about the robot:

[T-Mobile] is clear that those such as Huawei and Samsung are not only supplying TMO, but are also supplying their competitors such as Verizon, ATT, and other carriers.
1. If every Vendor is helped to establish TMO testing environment and standards, it would certainly also improve the product quality, etc. of each Vendor's competitors, which is equivalent to TMO doing a good deed for the industry.

2. TMO took about four years of time and lots of resource optimization to develop the Robot system, and it contains TMO's intellectual property rights.

3. TMO can provide a free testing environment for each Vendor, and it can ensure that this system only services TMO products. This only enhances the competitiveness of TMO.

26. On April 12, 2013, the HUAWEI USA Executive Director of Technical Acceptance also replied to the above email string, emphasizing that T-Mobile "strictly controlled" what the Huawei engineers could do in their lab, specifically that they "are limited to usage [of Tappy], and everything else is categorically denied." The email went on to state: "Due to answering headquarters' questions, our employees have had two complaints raised against them, and it was declared that if we inquired again, Huawei's credentials for using the TMO Robot Laboratory would end." The Executive Director of Technical Acceptance, echoing R.Y.'s prior suggestions, encouraged HUAWEI CHINA to send its own engineer to Seattle to gain direct access to Tappy.

D. The Thefts During May 2013.

27. HUAWEI CHINA decided to send its own engineer to Seattle, and designated F.W. to make the trip. On April 17, 2013, F.W. sent an email to the HUAWEI USA Executive Director of Technical Acceptance describing one of the goals of his upcoming trip as: "For the mechanical arm issues, go to the [T-Mobile] laboratory for reconnaissance and obtain measurement data." HUAWEI USA approved the travel and submitted paperwork to obtain a temporary visa for F.W. F.W. arrived in the United States on or about May 11, 2013.

28. On May 13, 2013, HUAWEI USA employees A.X. and H.L. improperly abused their badge access to allow F.W. into the T-Mobile laboratory where the Tappy
robot was located. A T-Mobile employee discovered that F.W. was in the laboratory without permission and told him to leave.

29. On the following day, May 14, 2013, F.W. returned to the T-Mobile laboratory, again without authorization. A.X. again improperly abused his badge access to allow F.W. into the laboratory. While inside the Tappy robot chamber, F.W. took numerous unauthorized photographs of Tappy, and otherwise gathered technical information about the robot, for the purpose of helping HUAWEI CHINA's development of the xDeviceRobot. A T-Mobile employee again discovered that F.W. was in the laboratory without permission and told him to leave.

30. On or about May 15 and 16, 2013, F.W. sent a series of emails to numerous employees of HUAWEI CHINA and HUAWEI USA, including the HUAWEI CHINA Director of Device Testing Management Department and the engineers working on the xDeviceRobot project. These emails contained multiple attachments, including photographs of the Tappy robot and related testing equipment that F.W. had taken inside the T-Mobile lab; and a document entitled “Robot Environmental Information,” which discussed in detail the mechanical assembly, operation, and other technical details of the Tappy robot as reflected in the photos and based on F.W.’s observations inside the T-Mobile lab. In one of the emails, F.W. stated, “I went once more today to TMO’s mechanical arm testing laboratory and gained an overall understanding of the test environment. I summarized it, please take a look,” referring to the attachments. F.W. further explained that T-Mobile had prohibited him from re-entering the laboratory, and that, moving forward, HUAWEI USA engineer A.X. would “help you get a deeper understanding of the remaining information.”

31. In light of F.W.’s misconduct in the laboratory, T-Mobile notified HUAWEI USA that its access to the Tappy laboratory was suspended and required HUAWEI USA to return all badges that had been issued to HUAWEI USA employees. T-Mobile agreed to allow one specific HUAWEI USA engineer, A.X., continued access
to the Tappy laboratory for limited testing related to particular Huawei phones that were
already scheduled for upcoming release.

32. On May 21, 2013, HUAWEI CHINA engineer J.Y. emailed HUAWEI
USA engineer A.X. (copying R.Y. and H.L.), directing him to provide information about
the specifications, operations, and componentry of the Tappy robot, including details
about the method of calculating the user interface response time; the shape, diameter, and
hardness of the capacitor pen tip; the calibration method and process of force control; the
sensors used to support the robotic arm and main camera; and “lots of photos and video
of test process.” On May 22, 2013, A.X. replied by email stating, “We’ll certainly help if
we can; this period is very sensitive,” referring to the fact that T-Mobile had restricted
HUAWEI USA’s access to the Tappy robot lab. On May 23, 2013, A.X. replied again
and provided some of the information requested in J.Y.’s email. In response to J.Y.’s
request for “lots of photos and video of test process,” A.X. stated, “After TMO gives
back our badges, I’ll send it back home. No need for home to keep reminding me.”

33. On or about May 29, 2013, a HUAWEI CHINA engineer emailed A.X. and
copied other HUAWEI CHINA engineers who were working on the xDeviceRobot
project (including J.Y. and F.W.). The HUAWEI CHINA engineer asked A.X. to
determine the diameter of a part of Tappy’s robot arm; specifically, the end tip of the
conductor stick.

34. Later on May 29, 2013, A.X. used his badge to access the T-Mobile Tappy
laboratory. As he was preparing to leave the laboratory, A.X. surreptitiously placed one
of the Tappy robot arms into his laptop bag and secretly removed it from the laboratory.
T-Mobile employees discovered the theft later that day, and contacted A.X. A.X. initially
falsely denied taking the robot arm, but then later claimed he had found it in his bag.
A.X. described the incident a “mistake” and offered to return the part. On the following
day, May 30, 2013, when the T-Mobile lab reopened, A.X. returned the stolen robot arm
to T-Mobile. T-Mobile thereafter revoked A.X.’s access to the laboratory and no longer
allowed any HUAWEI USA employees in the facility without an escort.
35. During the night of May 29-30, 2013, while A.X. had the stolen robot arm in his possession outside of the T-Mobile laboratory, F.W. took measurements of various aspects of the robot arm, including of the end tip of the conductor stick, and took photographs of the robot arm. Some of the photographs depicted the precise width of certain parts of the robot arm by showing a measuring device next to the parts. On or about May 29-30, 2013, F.W. sent these photographs as attachments via email to HUAWEI CHINA engineers including J.Y. F.W.'s email contained an explanation of multiple detailed measurements for various parts of the Tappy robot arm, including the end tip of the conductor stick, and how the various pieces were configured together. F.W.’s email concluded with, “See pictures for details.”

36. On or about May 30, 2013, A.X. participated in a conference call with multiple HUAWEI CHINA engineers who were involved with the xDeviceRobot project. On or about May 30-31, 2013, following up on issues discussed during the conference call, A.X. emailed multiple HUAWEI CHINA engineers, reporting the specific width of the tip of Tappy’s conductor stick and that F.W. had “obtained the probe.” In response, one of the HUAWEI CHINA engineers requested that A.X. obtain a more precise measurement of the conductor stick using a caliper device. A.X. replied that F.W. had “already sent the pictures home.”

E. Huawei’s Efforts to Cover-up its Thefts.

37. T-Mobile’s discovery of the theft of the robot part and F.W.’s unauthorized access of the laboratory caused great and immediate concern for HUAWEI CHINA and HUAWEI USA for several reasons. First, Huawei greatly valued its business relationship with T-Mobile, which was Huawei’s first significant customer in the United States wireless phone market. HUAWEI CHINA and HUAWEI USA were concerned that T-Mobile would terminate its relationship with them as a result of the incidents in the laboratory, thereby compromising Huawei’s ability to successfully enter the United States wireless phone market. Second, HUAWEI CHINA and HUAWEI USA were concerned about the potential for federal civil litigation. Specifically, HUAWEI CHINA...
and HUAWEI USA feared that T-Mobile would file a civil lawsuit against them in the United States District Court for the Western District of Washington, seeking monetary damages and other relief, as the result of their theft and related misconduct. Third, HUAWEI CHINA and HUAWEI USA were concerned that T-Mobile would refer the matter to federal law enforcement authorities, prompting a Federal grand jury investigation in the Western District of Washington.

38. Lastly, HUAWEI CHINA and HUAWEI USA were concerned about additional harm to Huawei’s reputation because the company had already been the subject of negative publicity regarding the company’s past practice of misappropriating proprietary business information and technology. For example, on October 2, 2012, the United States House of Representatives Permanent Select Committee on Intelligence issued a public report finding that Huawei posed a potential threat to national security, emphasizing, among other things, the company’s “pattern of disregard for the intellectual property rights of other entities and companies in the United States.” Moreover, the report stated that the Committee’s investigation had uncovered information that Huawei “may be violating United States laws” and “very serious allegations of illegal behavior” by Huawei, all of which the Committee would be referring to federal authorities “for potential investigation.” In addition, Huawei had been the subject of multiple lawsuits that had received negative public attention. In 2010, Motorola sued Huawei alleging that it had misappropriated Motorola’s proprietary wireless switching technology by acquiring it surreptitiously from Chinese Motorola engineers. In 2003, Cisco sued Huawei alleging that Huawei had stolen Cisco’s proprietary network router technology and related source code for use in Huawei’s own competing routers.

39. In light of all of these concerns, HUAWEI CHINA and HUAWEI USA attempted to affirmatively mislead T-Mobile about what had happened in T-Mobile’s laboratory. To that end, HUAWEI USA issued a 23-page “Investigation Report,” authored by its Chief Legal Counsel for Labor and Employment and its Executive Director of Human Resources. The report purported to summarize the findings of an
"internal investigation" into the above-described misconduct in the T-Mobile laboratory and related activities. In June 2013, as part of the "internal investigation,"

HUAWEI USA memorialized statements by HUAWEI USA and HUAWEI CHINA employees A.X. and F.W., and made them available for interviews with T-Mobile security personnel. During these interviews, A.X. and F.W. made false and misleading statements designed to conceal the full scope of Huawei's misconduct in attempting to steal T-Mobile's technology, including the extent to which other HUAWEI USA and HUAWEI CHINA employees were involved and the degree to which the Tappy technology had been compromised.

40. In emails sent on July 5, 2013, and August 9, 2013, the HUAWEI USA Executive Director of Human Resources informed T-Mobile that HUAWEI USA had "conducted our internal investigation here in the U.S.," and also that "Huawei HQ (China) has conducted a thorough investigation." The Executive Director represented that the investigations "confirmed" that A.X. and F.W. were "two individuals who acted on their own" and who "violated our Company's policies and thus they were both terminated for cause."

41. HUAWEI USA issued the formal Investigation Report on or about August 13, 2013. Shortly thereafter, in or about August or September 2013, HUAWEI USA provided T-Mobile with a redacted version of the Investigation Report. The Investigation Report contained several false and misleading statements about the events that had transpired. The report falsely stated that F.W. and A.X. had acted on their own, that their actions in May 2013 were "isolated incidents," and that the two "were lacking in their awareness of Huawei's cyber security policies." In fact, as HUAWEI USA and HUAWEI CHINA both well knew, the actions of F.W. and A.X. were undertaken at the direction of, and in coordination with, HUAWEI CHINA employees and were part of a months-long course of conduct to steal unauthorized technical information about Tappy.

42. The Investigation Report also stated that F.W. took nine photographs in the laboratory "[i]n a moment of indiscretion." The report intentionally omitted the fact that
HUAWEI CHINA and HUAWEI USA employees had secretly and deliberately taken unauthorized photographs of Tappy on multiple prior occasions, and that HUAWEI CHINA had issued numerous directives to HUAWEI USA to gather technical information about Tappy, and photographs of Tappy, for the purpose of developing Huawei's own xDeviceRobot.

43. The Investigation Report stated that F.W. sent only four photographs of Tappy to HUAWEI CHINA employees. The report intentionally omitted the fact that, after being caught in the T-Mobile laboratory for the second time, F.W. had circulated to HUAWEI CHINA engineers a six-page report containing technical information about Tappy, along with at least seven unauthorized photographs of the robot. The report also omitted the fact that even after F.W. had been barred from reentering the laboratory, he designated A.X. to provide HUAWEI CHINA engineers with a "deeper understanding of the remaining information" they were attempting to gather about Tappy.

44. The Investigation Report stated that, after A.X. had taken the robot part, he provided seven measurements of the part to a HUAWEI CHINA robotics engineer during a telephone call. The report intentionally omitted that, in the days preceding and following his theft of the robot part, A.X. also had exchanged multiple emails with HUAWEI CHINA robotics engineers, providing them technical information he had gathered about Tappy. The report also omitted that A.X. had previously taken unauthorized photographs of Tappy and sent the photographs to robotics engineers at HUAWEI CHINA.

45. On October 2, 2013, T-Mobile asked HUAWEI USA to provide them with any and all emails about Tappy that A.X. and F.W. had sent to other Huawei employees. HUAWEI USA declined to provide any such emails. On October 8, 2013, as part of HUAWEI CHINA's and HUAWEI USA's continuing cover-up, the HUAWEI USA Executive Director of Human Resources sent an email to T-Mobile stating: "Based on our findings, there are not a lot of emails corresponding between [A.X. and F.W.] and [HUAWEI CHINA] engineers that were related to [Tappy.] One or two of the emails
that remotely mentioned... the robot were related to the testing results between [Tappy] and the Huawei Testing.” In truth and in fact, there were numerous emails between HUAWEI CHINA robotics engineers and A.X. and F.W. pertaining to HUAWEI CHINA’s and HUAWEI USA’s efforts to steal unauthorized technical information about Tappy.

46. On or about May 5, 2014, T-Mobile sent HUAWEI USA a legal demand letter threatening to file a civil lawsuit against HUAWEI USA unless it paid T-Mobile monetary damages and took other remedial measures as the result of the theft and related misconduct. In response, in or about May 2014, HUAWEI USA produced the full, un-redacted Investigation Report to T-Mobile. Huawei in-house counsel also wrote letters to T-Mobile claiming that HUAWEI USA and HUAWEI CHINA had been “forthright” and had “cooperated” with T-Mobile after the events of May 2013, and representing that HUAWEI USA had provided to T-Mobile “many documents in regards to our internal investigation.” The letters from the Huawei attorneys also reiterated the false claim that A.X. and F.W. were “misguided” and had acted on their own without direction or involvement by other HUAWEI USA or HUAWEI CHINA employees.

47. On July 10, 2013, at the same time that HUAWEI CHINA and HUAWEI USA were falsely claiming that the conduct of A.X. and F.W. was “isolated,” constituted a “moment of indiscretion,” and was contrary to Huawei’s corporate polices, HUAWEI CHINA launched a formal policy instituting a bonus program to reward employees who stole confidential information from competitors. Under the policy, HUAWEI CHINA established a formal schedule for rewarding employees for stealing information from competitors based upon the confidential value of the information obtained. Employees were directed to post confidential information obtained from other companies on an internal Huawei website, or, in the case of especially sensitive information, to send an encrypted email to a special email mailbox. A “competition management group” was tasked with reviewing the submissions and awarding monthly bonuses to the employees who provided the most valuable stolen information. Biannual
awards also were made available to the top three regions that provided the most valuable information. The policy emphasized that no employees would be punished for taking actions in accordance with the policy.

48. The launch of this HUAWEI CHINA bonus program policy created a problem for HUAWEI USA because it was in the midst of trying to convince T-Mobile that the conduct in the laboratory was the product of rogue employees who acted on their own and contrary to Huawei’s policies. As a result, on July 12, 2013, the HUAWEI USA Executive Director of Human Resources sent an email to all HUAWEI USA employees addressing the bonus program. The email described the bonus program as:

“[I]ndicat[ing] that you are being encouraged and could possibly earn a monetary award for collecting confidential information regarding our competitors and sending it back to [HUAWEI CHINA].” The email went on to say: “[H]ere in the U.S.A. we do not condone nor engage in such activities and such a behavior is expressly prohibited by [HUAWEI USA’s] company policies.” The email did not state that the bonus program had been suspended by HUAWEI CHINA. Rather, the email emphasized that “in some foreign countries and regions such a directive and award program may be normal and within the usual course of business in that region.”

F. Tappy was Protected as a Trade Secret.

49. The Tappy robot system technology, as further described in paragraphs 3 and 4 above, including the information and know-how relating to the design, assembly, and operating methods of the T-Mobile testing robot; the specifications, source code, component selection, operating instructions, and other non-public elements of the robot technology; and proprietary combinations and implementations of the robot, contained and constituted trade secrets in that: T-Mobile took reasonable measures to keep such information secret; and the information derived independent economic value, actual and potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who could obtain economic value from the disclosure or use of the information.
G. Overt Acts in Furtherance of the Conspiracy.

50. During and in furtherance of the conspiracy, in Bellevue, within the Western District of Washington, and elsewhere, one or more of the conspirators committed one or more of the following overt acts, among others:

a. On or about September 10, 2012, H.P., the HUAWEI CHINA Director of Device Testing Management Department, sent an email directing HUAWEI USA employees to “figure out the [Tappy] Robot’s specifications and functions,” for the unauthorized purpose of furthering HUAWEI CHINA’s xDeviceRobot program.

b. On or about November 16, 2012, HUAWEI USA engineer A.X. sent an email to HUAWEI CHINA engineers containing multiple unauthorized photos of the Tappy robot and its software interface system that A.X. had taken inside of the secure T-Mobile lab, in violation of the nondisclosure agreements HUAWEI USA had signed.

c. On or about January 1, 2013, HUAWEI USA engineer A.X. sent an email to HUAWEI CHINA engineers containing confidential technical information about the Tappy robot and multiple unauthorized photos of the robot and its software interface system that A.X. had taken inside of the secure T-Mobile lab, in violation of the nondisclosure agreements HUAWEI USA had signed.

d. On or about April 12, 2013, R.Y., the HUAWEI USA Director of Technical Acceptance, sent an email to HUAWEI CHINA employees stating that HUAWEI USA had been unable to obtain the confidential technical information about Tappy that HUAWEI CHINA had been asking for, and suggesting that HUAWEI CHINA should send its own engineer to the United States who could access Tappy directly and thereby surreptitiously learn the information that HUAWEI CHINA was seeking.

e. On or about May 13, 2013, F.W., acting on behalf of HUAWEI CHINA, entered the T-Mobile robot laboratory, without authorization, for the purpose of obtaining technical information about the Tappy technology, for the unauthorized purpose of furthering HUAWEI CHINA’s robot program.
f. On or about May 14, 2013, F.W., acting on behalf of HUAWEI CHINA, entered the T-Mobile robot laboratory, without authorization, for the purpose of obtaining technical information about the Tappy technology, as well as taking unauthorized photographs of a Tappy robot, for the unauthorized purpose of furthering HUAWEI CHINA's robot program.

g. On or about May 29, 2013, A.X., acting on behalf of HUAWEI USA, and at the direction of HUAWEI CHINA, entered the T-Mobile robot laboratory for the purpose of stealing a Tappy robot part, without authorization, for the unauthorized purpose of furthering HUAWEI CHINA's robot program.

h. On or around August 13, 2013, HUAWEI USA generated an "Investigation Report" to provide to T-Mobile, as part of HUAWEI USA's and HUAWEI CHINA's efforts to conceal the conspiracy, including the extent to which the Tappy technology already had been compromised.

i. On or around October 8, 2013, the HUAWEI USA Executive Director of Human Resources emailed T-Mobile, misrepresenting the extent of email communications between A.X., F.W., and HUAWEI CHINA engineers that were related to Tappy, as part of HUAWEI USA's and HUAWEI CHINA's efforts to conceal the conspiracy, including the extent to which the Tappy technology already had been compromised.

All in violation of Title 18, United States Code, Sections 1832(a)(1), (a)(2), (a)(3), and (a)(5).

COUNT 2
(Attempted Theft of Trade Secrets)

51. Paragraphs 2 through 49 above are incorporated herein.

52. Between on or about April 12, 2013, and on or about May 31, 2013, at Bellevue, within the Western District of Washington, and elsewhere, HUAWEI DEVICE CO., LTD. and HUAWEI DEVICE USA, INC. attempted to:
(a) knowingly and without authorization steal, appropriate, take, carry away, and conceal trade secrets belonging to T-Mobile; and by fraud, artifice, and deception obtain trade secrets belonging to T-Mobile;

(b) knowingly and without authorization copy, duplicate, sketch, draw, photograph, download, replicate, transmit, deliver, send, communicate, and convey trade secrets belonging to T-Mobile; and

(c) knowingly receive, buy, and possess trade secrets belonging to T-Mobile, knowing the same to have been stolen, appropriated, obtained, and converted without authorization;

intending to convert a trade secret that is related to a product used and intended for use in interstate and foreign commerce, to the economic benefit of someone other than T-Mobile, and knowing that the offense would injure T-Mobile.

All in violation of Title 18, United States Code, Section 1832(a)(1)-(4).

**COUNTS 3-9**

(Wire Fraud)

53. Paragraphs 2 through 49 above are incorporated herein.

**A. The Scheme and Artifice to Defraud.**

54. Beginning at a time unknown, but no later than in or about June 2012, and continuing until on or about September 2, 2014, at Bellevue, within the Western District of Washington, and elsewhere, HUAWEI DEVICE CO., LTD. and HUAWEI DEVICE USA, INC. devised and intended to devise a scheme and artifice to defraud, and to obtain property by means of materially false and fraudulent pretenses, representations, promises, and the concealment of material facts.

55. The essence of the scheme and artifice to defraud was for HUAWEI DEVICE CO., LTD. and HUAWEI DEVICE USA, INC., through their employees, to access the Tappy robot laboratory for the unauthorized purpose of secretly obtaining technical information about the Tappy robot, on the false pretense and representation that only authorized activity would be conducted in the laboratory.
B. Manner and Means of the Scheme and Artifice to Defraud.

56. It was part of the scheme and artifice to defraud that HUAWEI DEVICE USA, INC. ("HUAWEI USA"), on behalf of itself and HUAWEI DEVICE CO., LTD. ("HUAWEI CHINA"), represented to T-Mobile in the aforementioned nondisclosure agreements that they would conduct only authorized activity within the Tappy robot laboratory, while intending that their employees would obtain confidential technical information about the Tappy technology, for the unauthorized purpose of furthering HUAWEI CHINA’s xDeviceRobot program.

57. It was part of the scheme and artifice to defraud that HUAWEI CHINA and HUAWEI USA, through their employees, represented to T-Mobile that they would conduct only authorized activity within the Tappy robot laboratory, and abide by the restrictions in the aforementioned nondisclosure agreements, each time one of their employees used a T-Mobile-issued access badge to gain entry to the laboratory.

58. It was part of the scheme and artifice to defraud that HUAWEI CHINA and HUAWEI USA used the limited access granted by T-Mobile to the Tappy robotic testing system to gather unauthorized confidential technical information about Tappy, for the purpose of furthering the development of Huawei’s xDeviceRobot, contrary to the promises and representations made by HUAWEI CHINA and HUAWEI USA to T-Mobile as described in paragraphs 56 and 57.

59. It was part of the scheme and artifice to defraud that HUAWEI CHINA and HUAWEI USA used the limited access granted by T-Mobile to the Tappy robotic testing system to take unauthorized photographs of Tappy, for the purpose of furthering the development of Huawei’s xDeviceRobot, contrary to the promises and representations made by HUAWEI CHINA and HUAWEI USA to T-Mobile as described in paragraphs 56 and 57.

60. It was part of the scheme and artifice to defraud that HUAWEI CHINA sent an employee to the United States in order to conduct reconnaissance on T-Mobile’s Tappy technology, for the purpose of furthering the development of Huawei’s
xDeviceRobot, contrary to the promises and representations made by HUAWEI CHINA and HUAWEI USA to T-Mobile as described in paragraphs 56 and 57.

61. It was part of the scheme and artifice to defraud that HUAWEI USA and HUAWEI CHINA stole, measured, and photographed a Tappy robot part, for the purpose of furthering the development of Huawei's xDeviceRobot, contrary to the promises and representations made by HUAWEI CHINA and HUAWEI USA to T-Mobile as described in paragraphs 56 and 57.

62. It was part of the scheme and artifice to defraud that HUAWEI CHINA and HUAWEI USA attempted to mislead T-Mobile through the “Investigation Report,” concealing the scope of their misconduct in attempting to steal T-Mobile’s technology, including the extent to which the technology had been compromised.

C. Execution of the Scheme and Artifice to Defraud.

63. On or about the dates set forth below, at Bellevue, within the Western District of Washington, and elsewhere, HUAWEI DEVICE CO., LTD. and HUAWEI DEVICE USA, INC., having devised the above-described scheme and artifice, for the purpose of executing this scheme and artifice, did knowingly transmit and cause to be transmitted by wire communication in interstate and foreign commerce writings, signs, signals, pictures, and sounds, to wit:

<table>
<thead>
<tr>
<th>Count</th>
<th>Date</th>
<th>Sender</th>
<th>Wire Transmission</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>April 12, 2013</td>
<td>HUAWEI USA</td>
<td>Email from the Western District of Washington to China discussing obtaining unauthorized technical information about Tappy</td>
</tr>
<tr>
<td>4</td>
<td>May 15, 2013</td>
<td>HUAWEI CHINA</td>
<td>Email from the Western District of Washington to China containing and discussing unauthorized photographs and other technical information gathered about Tappy</td>
</tr>
<tr>
<td>Date</td>
<td>Email from the Western District of Washington to China</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>May 16, 2013</td>
<td>Email from the Western District of Washington to China containing and discussing unauthorized photographs and other technical information gathered about Tappy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>May 23, 2013</td>
<td>Email from the Western District of Washington to China containing and discussing unauthorized technical information gathered about Tappy and discussing additional information to be gathered</td>
<td></td>
<td></td>
</tr>
<tr>
<td>May 29-30, 2013</td>
<td>Email from the Western District of Washington to China containing photographs, measurements, and other unauthorized technical information gathered about Tappy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>May 30-31, 2013</td>
<td>Email from the Western District of Washington to China containing and discussing unauthorized technical information gathered about Tappy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>October 8, 2013</td>
<td>Email from Texas to the Western District of Washington regarding the Investigation Report</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

All in violation of Title 18, United States Code, Sections 1343 and 2.

**COUNT 10**

(Obstruction of Justice)

64. Paragraphs 2 through 49 above are incorporated herein.

65. Beginning on or about June 1, 2013, and continuing through on or after September 2, 2014, at Bellevue, within the Western District of Washington, and elsewhere, HUAWEI DEVICE CO., LTD. and HUAWEI DEVICE USA, INC. attempted
to corruptly obstruct, influence, and impede an official proceeding, that is, the proceedings in *T-Mobile USA, Inc. v. Huawei Device USA, Inc.*, C14-1351RAJ, in the United States District Court for the Western District of Washington; and Federal grand jury proceedings in the Western District of Washington concerning HUAWEI DEVICE CO., LTD. and HUAWEI DEVICE USA, INC.

All in violation of Title 18, United States Code, Sections 1512(c)(2) and 2.

**ASSET FORFEITURE ALLEGATION**

66. The allegations contained in Counts 1-9 of this Indictment are hereby realleged and incorporated by reference for the purpose of alleging forfeiture pursuant to Title 18, United States Code, Section 2323(b); Title 18, United States Code, Section 981(a)(1)(C); and Title 28, United States Code, Section 2461(c).

**Counts 1-2**

67. Pursuant to Title 18, United States Code, Section 2323(b)(1), upon conviction of any of the offenses alleged in Counts 1-2 of this Indictment, the defendants, HUAWEI DEVICE CO., LTD. and HUAWEI DEVICE USA, INC., shall forfeit to the United States (1) any property used, or intended to be used, in any manner or part to commit or facilitate the commission of the offense and (2) any property constituting or derived from any proceeds obtained directly or indirectly as a result of the commission of the offense, including but not limited to a judgment for a sum of money representing the property described in this paragraph.

**Counts 3-9**

68. Pursuant to Title 18, United States Code, Sections 981(a)(1)(C), and Title 28, United States Code, Section 2461(c), upon conviction of any of the offenses alleged in Counts 3-9 of this Indictment, the defendants, HUAWEI DEVICE CO., LTD. and HUAWEI DEVICE USA, INC., shall forfeit to the United States any property, real or personal, which constitutes or is derived from proceeds traceable to the offense, including but not limited to a judgment for a sum of money representing the property described in this paragraph.
69. If any of the above described forfeitable property, as a result of any act or omission of the defendants,

   a. cannot be located upon the exercise of due diligence;
   b. has been transferred or sold to, or deposited with, a third party;
   c. has been placed beyond the jurisdiction of the Court;
   d. has been substantially diminished in value; or
   e. has been commingled with other property which cannot be divided without difficulty;

it is the intent of the United States, pursuant to Title 18, United States Code, Section 2323(b)(2); Title 21, United States Code, Section 853(p); and Title 28, United States Code, Section 2461(c), to seek the forfeiture of any other property of the defendants up to the value of the above-described forfeitable property.

A TRUE BILL:

DATED: 16 January 2019

Signature of foreperson redacted pursuant to the policy of the Judicial Conference of the United States

FOREPERSON

ANNETTE L. HAYES
United States Attorney

TODD GREENBERG
Assistant United States Attorney

THOMAS M. WOODS
Assistant United States Attorney
UNITED STATES OF AMERICA

v.

ZHENGQUAN ZHANG,
a/k/a "Zheng Quan Zhang,"
a/k/a "Jim Z. Zhang,"

Defendant.

SOUTHERN DISTRICT OF NEW YORK, ss.:

MICHAEL DENICOLA, being duly sworn, deposes and says that he is a Special Agent with the Federal Bureau of Investigation (the "FBI"), and charges as follows:

COUNT ONE
(Theft of Trade Secrets)

1. From at least in or about December 2016 through in or about March 2017, in the Southern District of New York and elsewhere, ZHENGQUAN ZHANG, a/k/a "Zheng Quan Zhang," a/k/a "Jim Z. Zhang," the defendant, with the intent to convert a trade secret that is related to a product and service used in and intended for use in interstate and foreign commerce, to the economic benefit of others than the owner thereof, and intending and knowing that the offense would injure the owner of that trade secret, knowingly did steal, and without authorization appropriate, take, carry away, and conceal, and by fraud, artifice and deception obtain such information; and without authorization did copy, duplicate, sketch, draw, photograph, download, upload, alter, destroy, photocopy, replicate, transmit, deliver, send, mail, communicate, and convey such information; and attempted to do so, to wit, ZHANG stole and attempted to convert to his own use the computer source code
underlying proprietary trading software, which was a trade secret of a financial services company for which ZHANG worked.

(Title 18, United States Code, Sections 1832 and 2.)

The bases for my knowledge and for the foregoing charges are, in part, as follows:

2. I am a Special Agent with the FBI, and I have been personally involved in the investigation of this matter. I have been a Special Agent with the FBI since approximately June 2015. Since becoming a Special Agent with the FBI, I have been assigned to a computer intrusion squad in the FBI’s New York Field Office. In that role, I have participated in numerous investigations of computer crimes, among other federal crimes. This affidavit is based upon my own observations, conversations with witnesses, and conversations with other law enforcement agents, as well as on my examination of reports and records prepared by others. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all of the facts that I have learned during the course of this investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

3. In the course of this investigation, I have spoken to representatives of a financial firm engaged in the trading of a variety of publicly traded securities and other financial products (“Firm-1”) and reviewed publicly available documents and records. Based on those conversations and that review, I am aware of the following information, in substance and in part, regarding the operations of Firm-1:

   a. Firm-1 acts as a market maker, facilitating trading and liquidity in a variety of financial markets. Firm-1 engages in billions of dollars of equities and fixed income trading on a daily basis.

   b. Firm-1 is headquartered in New York, New York and maintains offices and other facilities in various locations in the United States and abroad, including but not limited to an office in San Jose, California and a data center
in Purchase, New York. The majority of Firm-1’s employees are located at Firm-1’s New York headquarters.

4. In the course of this investigation, I have spoken to representatives of Firm-1 and reviewed internal Firm-1 documents and records. Based on those conversations and that review, I am aware of the following information, in substance and in part, regarding the trading operations of Firm-1:

a. A substantial portion of the trading done by Firm-1’s employees is facilitated by the use of Firm-1’s proprietary algorithmic trading models (collectively, the “Trading Models”). Firm-1 developed the Trading Models to, among other things, predict market movements and make trading decisions. Firm-1’s employees utilize the Trading Models in making trades involving publicly traded securities and other financial products in interstate commerce.

b. A substantial portion of the trading done by Firm-1’s employees is executed through the use of Firm-1’s proprietary trading platforms (collectively, the “Trading Platforms”). Firm-1 developed the Trading Platforms to, among other things, create orders and automatically submit those orders to an exchange or market center, as well as execute orders. Firm-1’s employees utilize the Trading Platforms in executing trades involving publicly traded securities and other financial products in interstate commerce.

c. The trading decisions resulting from Firm-1’s use of the Trading Models, and the efficiencies resulting from Firm-1’s use of the Trading Platforms, contribute substantially to Firm-1’s market share in the financial markets in which Firm-1 trades and to Firm-1’s overall trading profits. The competitive advantages and economic value that Firm-1 derives from the Trading Models and the Trading Platforms depend in part on their not being disclosed to a competitor or to the public.

d. Because of the proprietary nature of the Trading Models and the Trading Platforms, Firm-1 has put in place a variety of measures designed in part to protect the computer source code that comprises the Trading Models (the “Trading Models Source Code”) and the computer source code that comprises the Trading Platforms (the “Trading Platforms Source
Code") from disclosure to a competitor or to the public. For example:

i. The Trading Platforms Source Code is maintained in a software repository platform (the "Software Repository"). Firm-1 employees use a unique login identifier and password to log into the Software Repository. Within the Software Repository, only Firm-1 employees involved in the development or support of the Trading Platforms are permitted to access the Trading Platforms Source Code.

ii. The Trading Models Source Code is also maintained in the Software Repository. Firm-1 employees use a unique encryption key to encrypt and decrypt the Trading Models Source Code. Within the Software Repository, only Firm-1 employees involved in the development of the Trading Models are permitted to access the Trading Models Source Code. Moreover, those employees are given only certain encryption keys, in order to limit their access to a subset of the Trading Models.

iii. Firm-1 does not permit its employees to utilize external e-mail or file sharing websites on their work computers. Firm-1 further does not permit its employees to download data from their work computers to USB drives or other portable storage devices.

iv. Firm-1 employees sign agreements detailing, among other things, the confidential nature of Firm-1's work and Firm-1's ownership of work product developed in the course of that work.

v. Firm-1 employees are provided an employee handbook and a code of business conduct and ethics setting forth, among other things, Firm-1's requirements that employees maintain the confidentiality of non-public Firm-1 information and protect Firm-1's proprietary information, including its trade secrets and other intellectual property. Firm-1 employees acknowledge their agreement with such policies when they are hired and periodically during their employment.

5. In the course of this investigation, I have spoken to employees and representatives of Firm-1, including, among others, technical analysts employed by Firm-1. I have also reviewed various documents, including emails and communications, provided by Firm-1. Based on those
conversations and that review, I am aware of the following information, in substance and in part, regarding the employment of ZHENGQUAN ZHANG, a/k/a "Zheng Quan Zhang," a/k/a "Jim Z. Zhang," the defendant, by Firm-1:

a. Beginning in or about March 2010, ZHANG was employed by Firm-1 in technical roles within Firm-1. Although ZHANG initially worked out of Firm-1's offices in the greater New York City area, in or about November 2015, Firm-1 transferred ZHANG to its offices in San Jose, California, at his request.

b. Prior to December 2016, ZHANG was assigned to the technical operations and development operations group at Firm-1, which is responsible for, among other things, ensuring that the Trading Platforms and associated trading applications function correctly, and to address any issues that might arise. While working in that capacity, ZHANG was supervised by and reported to an individual employed by Firm-1 ("Individual-1").

c. Starting in December 2016, in addition to his work for the technical operations and development operations group at Firm-1, ZHANG also began working for the infrastructure group at Firm-1, which is responsible for, among other things, systems administration and troubleshooting server, network, and hardware issues as they arise. In order to facilitate his responsibilities as part of the infrastructure group, ZHANG was granted expanded access privileges to Firm-1 computers running a Unix-based operating system, which gave ZHANG access to, among other things, the Software Repository. ZHANG was not granted expanded access privileges to other Firm-1 computers running a Windows-based operating system.

d. On or about Saturday, March 25, 2017, an individual employed by Firm-1 as a quantitative analyst ("Analyst-1") logged in remotely to Analyst-1's computer desktop on Firm-1's Windows-based network. Analyst-1 specializes in performing research and programming to create Trading Models. Shortly after remotely logging into his computer desktop, Analyst-1's remote desktop session closed because another user had logged into the same remote desktop. Analyst-1 logged in again to the remote desktop, only to see that it appeared that another user had opened the file folder that held Analyst-1's archived email mailboxes. Analyst-1 continued to work remotely through the evening but was repeatedly disconnected due to
another user logging in. Analyst-1 was able to ascertain the 
unique identifier associated with the other user who was logging 
into Analyst-1’s remote desktop.

e. On or about Sunday, March 26, 2017, Analyst-1 notified Firm-1’s network security group of this unusual 
activity, and provided the unique identifier that Analyst-1 had 
observed logging in to Analyst-1’s remote desktop. Using that 
identifier, Firm-1’s network security group determined that 
ZHANG had been accessing Analyst-1’s remote desktop without 
authorization. Firm-1 then disconnected all computer access 
privileges for ZHANG.

f. Early in the morning on or about Monday, 
March 27, 2017, ZHANG sent an email to Individual-1, in which 
ZHANG wrote, in part, that ZHANG had determined that his Windows 
account had been terminated, which he knew “would happen because 
[of] what I did in the past few days and Saturday. I am still 
questioning myself why I did that.” ZHANG further stated that 
on Saturday, he had “remotely logged in a few desktops randomly 
without authorization, using [his] Mac laptop.” ZHANG explained 
that he was able to do so because he had modified (without 
authorization from Firm-1) a specific web application used by 
Firm-1 employees so that ZHANG could capture individual users’ 
logins and passwords. ZHANG stated that he had done so because 
he was aware of a potential acquisition of Firm-1, which he 
believed might place his job at risk, and that he sought to 
understand the status of the company through gaining access to 
these users’ accounts.

g. Later that day, ZHANG sent a text message to 
Individual-1, stating in part that he was about to go to the 
office “to hear [the] verdict” and asking if Individual-1 was 
available to speak. Individual-1 and ZHANG then had a telephone 
conversation, in which ZHANG admitted to Individual-1 that he 
had also accessed the remote desktop of another quantitative 
analyst based in Firm-1’s headquarters in New York City 
(“Analyst-2”).

6. In the course of this investigation, I have 
spoken to employees and representatives of Firm-1, including, 
among others, technical analysts employed by Firm-1. Based on 
those conversations, I am aware of the following information, in 
substance and in part, regarding Firm-1’s subsequent broader
investigation of the activities of ZHENGQUAN ZHANG, a/k/a "Zheng Quan Zhang," a/k/a "Jim Z. Zhang," the defendant:

a. In the course of its investigation of ZHANG, Firm-1 has reviewed various data relating to ZHANG’s computer activity. Pursuant to that review, Firm-1 has found evidence that ZHANG successfully exfiltrated the source code for multiple Trading Models and Trading Platforms to a third-party software development site (the "Development Website"). Firm-1 has found evidence that ZHANG’s efforts to steal this data began at least as early as December 2016.

b. Firm-1’s technical staff determined that ZHANG installed on Firm-1’s systems computer code designed to look for encryption keys on the servers used to build the Trading Models. Doing so would have enabled ZHANG to gain access to much larger portions, if not the entirety, of the Trading Models Source Code.

c. In addition, Firm-1 identified an area of its computer networks where ZHANG stored data - over 3 million files - prior to uploading it onto the Development Website. Firm-1’s review of that data shows, among other things, that ZHANG gained unauthorized access to unencrypted portions of the Trading Models Source Code.

d. In addition, Firm-1 identified computer code that ZHANG had written to exfiltrate data to the Development Website. Firm-1’s review of that data shows, among other things, that ZHANG uploaded to the Development Website unencrypted portions of the Trading Models Source Code, as well as email mailbox files assigned to the head of the quantitative side of Firm-1’s market making group. ZHANG also accessed the Development Website thousands of times from Firm-1’s networks.

e. All communications between Firm-1’s computer network and the external internet pass through a proxy server. Firm-1’s primary proxy server is maintained by a third-party vendor. Firm-1’s backup proxy server is maintained at Firm-1’s data center in Purchase, New York. The computer code that ZHANG wrote to exfiltrate data to the Development Website was designed to route all of the data through Firm-1’s backup proxy server in Purchase, New York.
WHEREFORE, I respectfully request that an arrest warrant be issued for ZHENGQUAN ZHANG, a/k/a "Zheng Quan Zhang," a/k/a "Jim Z. Zhang," the defendant, and that ZHANG be arrested and imprisoned or bailed, as the case may be.

MICHAEL DENICOLA
Special Agent
Federal Bureau of Investigation

Sworn to before me this 3rd day of April, 2017

THE HONORABLE ANDREW J. PECK
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK
CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of July 5, 2018 in the county of Schenectady in the Northern District of New York, the defendant(s) violated:

<table>
<thead>
<tr>
<th>Code Section</th>
<th>Offense Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Count 1: 18 U.S.C. § 1832(a)(1)</td>
<td>Theft of Trade Secrets</td>
</tr>
</tbody>
</table>

This criminal complaint is based on these facts:

✔ Continued on the attached sheet.

Sworn to before me and signed in my presence.

Date: August 1, 2018

City and state: Albany, New York

Complainant’s signature

FBI S/A M.D. McDonald

Printed name and title

Judge’s signature

Hon. Christian F. Hummel, U.S. Magistrate Judge

Printed name and title
AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

STATE OF NEW YORK

) cc

COUNTY OF ALBANY

I, M.D. McDonald, being duly sworn, depose and state that:

INTRODUCTION

Agent Background

1. I have been employed as a Special Agent of the FBI since 2002 and currently I am assigned to the Albany, NY field office where I work on the Counterintelligence Squad. During my 16 years of employment with the FBI, I have received training on investigative techniques and evidence recovery procedures, I have conducted many criminal investigations, and I have conducted many searches and arrests. I was employed for approximately 8 years (from 2011 through 2018) as a Supervisory Special Agent and Associate Division Counsel, where I oversaw the legal, ethics, and asset forfeiture programs for the Albany field office.

2. I am a licensed attorney and member of the Bar of the State of New York, having graduated from Albany Law School of Union University and admitted to the New York State Bar in 1998. During my 20 years as a lawyer, I have completed many continuing legal education courses of instruction, including courses focusing on ethics and criminal practice, and maintained my good standing as a licensed attorney.

3. I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in Title 18, United States Code, Section 2516(1). As a FBI Special Agent, I am authorized to seek and execute federal arrest and search warrants for Title 18 criminal offenses, including offenses related to the theft of trade secrets.

4. In accordance with my present duties, I make this affidavit in support of a criminal complaint charging Xiaqing Zheng with a violation of 18 U.S.C. § 1832(a)(1) [Theft of Trade Secrets].

5. I make this affidavit from personal knowledge based on my participation in this investigation, and review of reports by myself and/or other law enforcement agents, communication with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience. The information outlined below is provided for the limited purpose of establishing probable cause and does not contain all details or all facts of which I am aware relating to this investigation.
SUMMARY OF THE INVESTIGATION

6. The trade secret(s) at issue in this case belong to General Electric's Power division and involves mathematical computations relating to sealing and optimization of turbines, in the form of MatLab (a high level computer language used for mathematical computing) and Excel (spreadsheet) files. GE considers this technology to be proprietary and has taken steps to keep its technology secret.

7. Xiaqing Zheng, a Principal Engineer employed by GE at its GE Power facility in Schenectady, NY, is suspected of taking/stealing, on multiple occasions via sophisticated means, data files from GE's laboratories that contain GE's trade secret information involving turbine technology. In particular, Zheng is believed to have utilized elaborate means to conceal his removal of GE data files including conducting his activities after normal work hours, "staging" encrypted files in folders on his work (desktop) computer, using encryption to prevent GE from seeing the contents of the data files, using steganography to (in essence) hide data files in the binary code of another file (specifically a digital photograph), and e-mailing GE's data files to Zheng's personal e-mail address ----------------@hotmail.com.¹

8. Although the overall investigation relates to a broader scope of activities involving the suspected theft and unlawful use of GE's trade secrets, including Zheng's ownership interest in companies that may compete with GE and Zheng's contacts in China, the primary focus of this affidavit is Zheng's actions in 2018 in which he encrypted GE data files containing trade secret information, and thereafter sent the trade secret information from his GE work (desktop) computer to Zheng's personal e-mail address (----------------@hotmail.com) hidden in the binary code of a digital photograph via a process known as steganography. Additionally, the secondary focus of this affidavit is Zheng's actions in 2014 in which he downloaded more than 19,000 files from GE's computer network onto an external storage device, believed by GE investigators to have been a personal thumb drive.

DETAILS OF THE INVESTIGATION

Background on Xiaqing Zheng

9. Xiaqing Zheng is a 56 year old U.S. citizen of Chinese descent. Zheng is also believed to have Chinese citizenship and to possess significant personal and professional contacts in China. Zheng has lived with his wife at their marital residence in Niskayuna, New York for several years. Zheng has degrees from Northwestern Polytechnical University and Massachusetts Institute of Technology in "aero engine" fields.

10. Zheng was hired by General Electric in 2008 to work as a Principal Engineer. Since being hired, Zheng has worked, full time, for GE's Power division in Schenectady County, NY. Zheng works on "Steam Turbine Flow Path" technology. This technology is used in many of the turbines that GE sells both domestically and internationally. In order to perform his duties, Zheng has been given a GE-issued laptop computer, a GE-issued desktop computer, a GE-issued smartphone (an iPhone), and a GE e-mail address. GE employees like Zheng are permitted to,

¹ Zheng's actual Hotmail e-mail address is available to the Court upon request.
and routinely do, take their GE-issued electronics home in order to work. Additionally, Zheng has disclosed to GE that he maintains a personal e-mail address of __________@hotmail.com.

11. According to GE, Zheng is the owner of a business entity (opened in 2015) called Nanjing Tainyi Aeronautical Technology, Ltd, located in Nanjing, China. Zheng disclosed this information to GE, and also disclosed to GE that he and “his brothers” own the company. Zheng has described the business as a “parts supplier for civil aviation engines.”

12. GE has conducted a conflict of interest analysis over Zheng’s Chinese company and determined that Zheng’s company posed at least three potential conflicts: (i) the company could sell parts to GE Aviation (a subsidiary of GE); (ii) the company could sell parts in competition to GE Aviation; and (iii) Zheng’s time spent working for his company could make him a less productive employee for GE. GE determined that Zheng’s “role is obviously more than just “owner” – he is responsible for development and implementation of new sealing technologies for his company.” However, GE did not instruct Zheng that his interest in the Chinese company was unacceptable, and Zheng was permitted to retain his GE employment.

Publicly Available Information on Zheng’s Chinese Companies

13. Although I am unable to determine much about Zheng’s company due to its location in China, a basic level Internet search shows that Zheng is (i) the “owner” and “chairman” of (a slightly differently named company) Tianyi Aviation Technology Co, Ltd., and (ii) the “general manager” of a separate company Lioning Tianyi Aviation Technology Co Ltd. According to publicly available Internet postings, Zheng’s Chinese companies “fill gaps” in technical fields in China in the aviation industry. According to some of the same postings, Zheng himself is described as a leader of a team of experts, and a person who has been involved in opening an industrial facility in China. Also according to the publicly available postings, Zheng was described as a 2012 selectee of the “Thousand Talents Program”. I know this program to be a Chinese government program designed to recruit highly educated researchers to bring their skills to China.

14. GE has noted that based on their review of the publicly available Internet sites relating to Zheng’s companies in China, it appeared he was working on the same types of technology for the Chinese companies that he is employed to work on by GE. The GE proprietary technologies on which Zheng works would have economic value to any of GE’s business competitors.

15. I reviewed publicly available publications on the Internet website tianyiseal.com, relating to Tianyi Aviation Technology, Co, and I observed a publication about the company’s efforts toward developing advanced turbine sealing technology. On the web page is a posting that reads, in pertinent part, “Sealing technology is the most effective way to improve engine efficiency... Low leakage advanced seals could cut in half the estimated 4% cycle air currently used to purge high pressure turbine cavities... It is a goal of NTAT to develop efficient manufacture technology to serve engine companies with low-cost, high-quality sealing products.” In essence, a company that Zheng appears to either own or manage is advertising in China its expertise in turbine sealing technology – the technology on which Zheng works on at
GE, and the technology that Zheng is believed to have egressed from GE’s system while encrypted and hidden in a photograph.

**GE Has Taken Steps to Protect its Turbine Sealing Trade Secrets**

16. GE Power has taken substantial steps toward protecting its trade secret information relating to its turbine technologies. GE Power’s facilities (at which Zheng works, and where Zheng encrypted the MatLab and Excel files, moved them to a “temp folder, renamed them, hid them within the binary code of his digital photograph, and e-mailed them to his personal Hotmail address) are access controlled utilizing perimeter security, as well as internal access control security. Visitors are required to register with security, wear visitor badges, and be escorted by approved personnel. Zheng has full access to the GE space in the GE Power facility. GE employees are required to sign proprietary information agreements, and they are advised of GE policies including the fact that any inventions or innovations they may create while a GE employee are the property of GE. Additionally all employees are subject to the GE Acceptable Use of GE Information Resources (AUGIR) which explains how to use and protect GE information.

17. To protect their sensitive data / trade secrets, GE employs multiple digital controls, including:

a. **Access Control** – GE computing assets are protected by a centrally managed network/host login and authentication credentials. These credentials are granted to authorized employees and contingent workers based on their need to access company data.

b. **Banner warnings** – GE computer systems contain banner style warning notices to advise GE employees that GE’s computer system is available to them for work-related reasons and is subject to monitoring. GE advises employees that GE monitors employees’ usage of its computer systems (which I and GE believe is the main reason Zheng encrypted the files he stored in temp folders on his computer, as GE would have been able to view the files Zheng was staging for egress had he left the files unencrypted).

c. **Ban on use of USB drives** – In 2016 or 2017, GE instituted a policy restricting employees’ use of external USB drives such as thumb drives, and GE took steps to ensure their computer system would not permit the use of thumb drives. This security measure prevents employees from downloading trade secret information to drives they could physically take with them (which is a reason why I and GE believe Zheng employed the complex measures he used to hide trade secret information in a digital photograph and utilize e-mail to egress it, as he could no longer utilize a thumb drive).

18. GE Power has general office policies on the use and handling of its confidential and proprietary information which are set out, for example, during training, in employee handbooks, through oral warnings at company meetings or conventions, and on signs or banners posted in
the workplace. GE has told me that it was clear to Zheng that he was not authorized to take the files he took, and that the files were undoubtedly GE’s property. GE believes Zheng used such a complex process to encrypt, stage, hide and e-mail the MatLab and Excel files specifically because it was very clear that he was not permitted to take this data, and there was no plausible reason to go to such lengths to hide what he was doing if he believed the files were not trade secrets that he was not permitted to take or share with third parties.

**GE’s Identification of the Crimes Under Investigation**

19. In 2014, GE corporate security learned that Zheng had copied 19,020 electronic files from one of his GE-issued computers onto a USB external storage device, believed to be a thumb drive. GE has been unable to determine the contents of the 19,020 files, however, it is suspected that the files related to Zheng’s work for GE as employees are discouraged from using GE-issued electronics to conduct anything more than incidental personal business. GE investigators interviewed Zheng in 2014 regarding this incident, and Zheng told them that he had deleted the files. GE had no additional information about the downloaded files, nor any corroboration about whether the files had been deleted or shared with any third parties.

20. In November – December 2017, GE discovered that approximately 400 encrypted files had been saved on Zheng’s work (desktop) computer. The files were encrypted using a program called Axcrypt – a program not used by GE. This practice was not standard for GE employees, and GE did not know why Zheng would be encrypting files on his work (desktop) computer. Due to the encryption, GE was unable to view the contents of the 400 files that Zheng encrypted and saved on his GE computer.

**GE’s Efforts to Monitor Zheng’s Computer Activity**

21. Following GE’s discovery of the 400 encrypted files on Zheng’s GE-issued computer, GE installed monitoring software on Zheng’s computer(s) in an attempt to determine what information he was encrypting, and what he was doing with the information (e.g., transferring it elsewhere, etc.).

22. During the process of monitoring Zheng’s activities on his computer(s), GE discovered that on or about July 5, 2018 Zheng moved approximately 40 encrypted files to a “temp folder” on his GE-issued work (desktop) computer. Since GE security personnel were monitoring Zheng’s activities they were able to determine the password Zheng used for the encryption. GE determined that the files were MatLab and Excel files containing calculations relating to sealing and optimizing turbine technology – information that GE considers to be proprietary and secret.

23. In connection with GE’s monitoring of Zheng’s computer activities, GE learned that on July 5, 2018 Zheng used “steganography” (a means of hiding a data file within the code of another data file) to conceal data from the aforementioned 40 electronic files onto his GE-issued work (desktop) computer. Through the steganography technique, Zheng placed the aforementioned electronic files into the binary code of an innocuous looking separate electronic file on the computer - a digital photograph of a sunset. Zheng then e-mailed (using his GE e-mail address) the digital photograph file of the sunset (which secretly contained the hidden GE
electronic files containing GE’s proprietary data) to his personal e-mail address of -----------@hotmail.com. This action is detailed more thoroughly below in the portion of this Affidavit labeled “Steganography Egress Summary”.

**Steganography Egress Summary**

24. On Thursday, July 5, 2018, at around 11:12 a.m., Zheng compressed 39 MatLab electronic files (MatLab is a computer programming language used for technical computing) and one Excel (spreadsheet) file into a new electronic file titled ‘Optimizing.zip’. This activity occurred within file system path d:\users\204050598\documents\unt\2018\carbon\design tool\.

25. Then, using the software application Axcrypt (encryption software), Zheng encrypted the electronic file ‘Optimizing.zip’. To do so he used a personal passphrase (NJJ9*UHB).

26. Next, using Axcrypt, Zheng renamed the encrypted file ‘‘Optimizing.zip.axx’ to ‘F03B336A.axx’ . According to GE, the word “optimizing” would appear to relate to turbine optimizing, which would seem to be work related files, but ‘F03B336A’ was not a file name that would have any connection to GE’s proprietary trade secret information, so essentially Zheng used an innocent-looking name for the file.

27. Zheng then cut the encrypted file ‘F03B336A.axx.’ from d:\users\204050598\documents\unt\2018\carbon\design tool\ and pasted it into c:\tmp (described as a “temp” folder).

28. Around 5:17 p.m. on July 5, 2018, Zheng plugged an iPhone into his GE-issued work (desktop) computer. Zheng copied an image file ‘IMG_2064.JPG’ from the iPhone onto the desktop of his GE-issued work computer. Zheng then renamed this image as ‘dawn.JPG’.

29. Zheng edited the ‘dawn.JPG’ (originally just a photograph of a sunrise or sunset with no text) image by typing “Happy Fourth of July” into the image. Zheng re-saved the image to the desktop of his GE-issued work computer. Zheng then cut the file from the desktop of his GE-issued work computer and pasted it into c:\tmp (the same folder in which Zheng had saved the 39 MatLab files and one Excel file).

30. Zheng then opened Cygwin Bash Shell (a text-style layer of computer programming language that understands and executes commands typed by users) and typed the commands “cd c:\tmp” and “dir” which listed the contents of the directory on the command line interface. Zheng then typed “vim -b dawn.jpg” which listed the binary code (essentially the “ones and zeros” used in computer programming) of the ‘dawn.JPG’ file. Zheng then typed in “88” at the end of the binary code. Next, Zheng typed “r: F03B336A.axx” which inserted a read-only copy of this encrypted file into the binary code of the ‘dawn.JPG’ file. Zheng then added “88” at the end of the new binary code. Essentially in this process, Zheng pasted the binary code for the 39 MatLab files and one Excel file (most, if not all, of which contained GE’s proprietary information) at the end of the binary code for the digital photograph, with “88” (which I know to be widely viewed as a lucky number and symbol of good fortune in Chinese culture), thereby setting the GE-owned data apart from the innocent-looking digital photograph data.
31. Zheng returned to the Explorer Window within the c:\tmp and renamed the file ‘F03B336A.axx’ to ‘de.dat’, then shredded and deleted the file through the AxCrypt application. Changing the .axx (Axcrypt) file extension to .dat (data file) extension is significant, as GE explained that a .dat file would seem to be a routine file type that would not draw attention. Through this process, Zheng deleted the data from his “temp” folder, as the data had been hidden in the binary code of the digital photograph.

32. At 5:29 p.m. on July 5, 2018, Zheng attached the file “dawn.JPG” to a message in his GE Outlook e-mail account, typed “Nice view to keep” into the subject line of the e-mail, and sent the e-mail with the attachment from his GE e-mail address to ----------@hotmail.com. In this process, Zheng sent the digital photograph (with the GE-owned files hidden in the binary code) to his personal e-mail address – completing the process of “egressing” or taking the GE-owned proprietary information from the GE computer system and sending it to his Hotmail account, stored on Microsoft Online Services’ servers where he could retrieve it from an outside location.

33. In essence, Zheng took great care to conceal what he was doing with GE’s proprietary data files, and he not only hid the data he was staging in a “temp folder” by encrypting it so GE could not see what files he was saving, but he also used steganography to hide the fact that he sent GE’s data to his personal e-mail address (i.e. concealing the data within the binary code of the digital photograph). A person tasked by GE with routine e-mail monitoring would have seen the digital photograph in Zheng’s GE e-mail, but unless he/she knew where to look within the binary code of the digital photograph, he/she would only have seen a photograph of a sunset. Zheng’s use of encryption and steganography techniques are both uncommon and serve no apparent purpose but for concealing his activities from his employer.

34. Zheng’s actions (moving the files, renaming them, encrypting them, and hiding them within the binary code of seemingly harmless files) are uncommon even among trained computer experts, and both GE Digital analysts and FBI agents specializing in cyber crimes have told me that they were aware of these measures in theory, but that they had never actually seen a subject employ them. GE provided investigators real-time video of Zheng’s computer activities on July 5, 2018, and the entire process took Zheng less than 10 minutes. Based on my experience and training, including my discussions with FBI Agents who specialize in cyber crimes, the fact that Zheng accomplished this complex process so quickly and easily makes it highly probable that he had practiced these techniques and utilized them in the past.

35. According to GE, Zheng is in possession of at least the following mobile electronic items: an HP Elite Laptop computer and an iPhone X. And, according to GE, Zheng downloaded over 19,000 files from the GE computer system onto an external USB device, believed by GE to be a thumb drive.

Common Practices Involving Stolen Trade Secrets

36. Based on my training and experience, I am aware that once trade secret information / data is egressed from the lawful owner’s computer system (e.g. on a thumb drive or via e-mail), the stolen trade secret information can easily be stored and saved on a wide variety of electronic storage devices such as laptop or desktop computers, cellular telephones, iPads or similar tablet
style devices, thumb drives, and other devices containing electronic storage capabilities. Once the stolen trade secret information has been egressed, the information can be used by, sold to, exchanged with, traded to, etc. individuals and entities who are looking to illegitimately acquire the information.

37. Based on my training and experience, I know that there is a market in China comprised of individuals and businesses who are willing to pay money for trade secret information/data stolen from U.S. companies. Some of these individuals and businesses are willing to pay more money than others, thus an individual who first possesses stolen trade secret information may ‘shop’ the stolen trade secret information in an effort to obtain the most money. Such an individual’s ‘shopping’ of the stolen trade secret information takes time and requires the individual to maintain the stolen trade secret information in a format that preserves the stolen information.

Execution of a Search Warrant at Zheng’s Niskayuna, New York Residence

38. On August 1, 2018, agents with the FBI executed a federal search warrant at Zheng’s residence in Niskayuna, New York. Agents were authorized to search for, and seize, evidence involving the theft of trade secrets from GE.

39. In connection with the above-referenced search, agents seized:
   
a.) a handbook that explains the type of resources the government of China will give to individuals or entities who can provide certain technologies;

b.) Zheng’s passport showing five international trips to China in the past two years; and

c.) various electronic items of which forensic examination is beginning.

Interview of Xiaqing Zheng

40. On August 1, 2018, agents with the FBI interviewed Zheng during the execution of the search warrant for his residence. During the interview Zheng made a number of oral statements, including, in sum and substance:

   a.) that it was common knowledge that “MatLab” electronic files are General Electric’s (GE’s) property and that it would be unlawful to take such files without permission;

   b.) that it is normally very difficult to unlawfully take any of GE’s proprietary property;

   c.) that despite the difficulties inherent in attempting to unlawfully take GE’s property, he used the steganography process on July 5, 2018 to take multiple electronic files belonging to GE that contained data about turbine technology;

   d.) that he had previously used steganography on somewhere around 5-10 prior occasions to take materials that belonged to GE;
e.) that the companies in China that he owns or works for work on the same technologies that he works on as GE engineer; and

f.) that his companies in China are not yet profitable, but have received grant money / funding from the government of China.

**OFFENSE ALLEGED**

41. Based upon my experience, training, and the totality of circumstances in the above information, there is probable cause to believe that:

   a.) On or about July 5, 2018, in the Northern District of New York, Xiaoqing Zheng, the defendant, with the intent to convert a trade secret that is related to a product and service used in and intended for use in interstate and foreign commerce, specifically “Steam Turbine Path Flow” technology, to the economic benefit of a person, or persons, other than the trade secret’s owner, and knowing that the offense will injure any owner of that trade secret, knowingly did steal such information, all in violation of 18 U.S.C. § 1832(a)(1).

Sworn and subscribed to before me on this ___ day of August, 2018.

The Honorable Christian F. Hummel
United States Magistrate Judge
Northern District of New York
CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of April 30, 2018 in the county of Santa Clara in the Northern District of California, the defendant(s) violated:

<table>
<thead>
<tr>
<th>Code Section</th>
<th>Offense Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>18 U.S.C. § 1832(a)(1)</td>
<td>Theft of Trade Secrets</td>
</tr>
</tbody>
</table>

This criminal complaint is based on these facts:

See attached affidavit of S/A Eric Proudfoot

PENALTIES: 10 years imprisonment, $250,000 fine, $100 special assessment, and 3 years' supervised release

Continued on the attached sheet.

Continued on the attached sheet.

Sworn to before me and signed in my presence.

Date: July 9, 2018

City and state: San Jose, California

Virginia K. DeMarchi, U.S. Magistrate Judge
AFFIDAVIT PRESENTED IN SUPPORT FOR A CRIMINAL COMPLAINT

I, Eric M. Proudfoot, Special Agent of the Federal Bureau of Investigation ("FBI"), being duly sworn, hereby declare as follows:

INTRODUCTION AND AGENT BACKGROUND

1. This affidavit is presented in support of a criminal complaint charging Xiaolang Zhang ("Zhang") with the crime of theft of trade secrets, in violation of Title 18, United States Code, Section 1832, Theft of Trade Secrets.

2. I am an "investigative or law enforcement officer of the United States" within the meaning of Section 2510(7) of Title 18, United States Code, that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Title 18, United States Code, Section 1832.

3. I have been employed as a Special Agent of the Federal Bureau of Investigation since March 2, 2008, and am currently assigned to the San Francisco Division. While employed by the Federal Bureau of Investigation, I have investigated federal criminal violations related to high technology/cybercrime, child exploitation, child pornography, foreign counterintelligence, and intellectual property crime. I have gained experience through training at the Federal Bureau of Investigation and everyday work relating to conducting these types of investigations. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

4. As an FBI agent, I am authorized to investigate violations of United States law and I am a law enforcement officer with the authority to execute warrants issued under the authority of the United States. During my career as a Special Agent of the FBI, I have received training and possess actual experience relating to Federal criminal procedures and Federal statutes. I have
also received specialized training and instruction in the field of investigation in computer-related crimes. I have had the opportunity to conduct, coordinate, and participate in numerous investigations relating to computer-related crimes. I have participated in the execution of numerous search warrants conducted by the FBI and have participated in the seizure of email accounts and computer systems.

5. The facts in this affidavit are based on my personal participation in this investigation, my training and experience, and documents, records, emails, and other types of information obtained during the investigation from other sources and witnesses. The FBI has, thus far conducted interviews and reviewed documentation provided by the victim company, Apple, ("Apple"), which included file listings, closed circuit television images, physical access badge history, and employee agreements. The FBI has also conducted a physical search of ZHANG's residence, authorized on June 22, 2018, by the Honorable Susan van Keulen, Magistrate Judge, United States District Court, Northern District of California, San Jose Division. Because this affidavit is being submitted for the limited purpose of securing a criminal complaint, I have not included every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of violations of U.S. law occurred. Also, where I refer to conversations and events, I often refer to them in substance and in relevant part rather than in their entirety or verbatim, and figures and calculations set forth in this complaint are approximate, unless otherwise noted.

APPPLICABLE STATUTES

6. The FBI is investigating alleged violations of Title 18, United States Code, Section 1832, which states in part:

(a) Whoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the
economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly—
(1) Steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;
(2) Without authorization copies, duplicates, ... downloads, uploads, ... replicates, transmits, delivers, sends, mails, communicates, or conveys such information;
(3) Receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;
(4) Attempts to commit any offense described in paragraphs (1) through (3) . . .
(5) Conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,
shall . . . be fined under this title or imprisoned not more than 10 years, or both.

ENTITIES

7. Apple, Inc. “Apple” is a technology company headquartered in Cupertino, California with an annual revenue (in 2017) of $229 billion.

8. Xiaopeng Motors, aka Xpeng Motors, (“XMotors”) is an intelligent electric vehicle company with headquarters in Guangzhou, China, and North American offices located in Palo Alto, California.

INDIVIDUALS

9. Xiaolang Zhang (“ZHANG”) is a former Apple employee, working as a hardware engineer on their autonomous vehicle development team.

ZHANG BACKGROUND

10. ZHANG was hired at Apple starting on December 7, 2015, to work on a project to develop software and hardware for use in autonomous vehicles (the Project). Although Apple has made general statements to the press about being interested in autonomous vehicle development, the details of Apple’s research and development for the Project is a closely
guarded secret that has never been publicly revealed. Most recently, ZHANG worked on the Compute Team, where he designed and tested circuit boards to analyze sensor data within the Project. Because of his role on the team, ZHANG was granted broad access to secure and confidential internal databases containing trade secrets and intellectual property for the Project. Among these are multiple confidential databases whose names and categories are known to the government (the “Databases”).

11. ZHANG took paternity (new parent) leave following the birth of his child from April 1 to April 28, 2018, pursuant to Apple’s employee leave policy. While on paternity leave, ZHANG traveled with his family to China. On April 30, 2018, shortly after returning from China, ZHANG met with his immediate supervisor at Apple, and explained that ZHANG would be resigning to move back to China in order to be closer to his mother who he stated was in poor health. As the meeting progressed, ZHANG disclosed that he intended to work for XMOTORS — a Chinese start-up company focused on electric automobiles and autonomous vehicle technology.

12. After hearing ZHANG’s intentions and feeling that he had been evasive during their meeting, ZHANG’s supervisor asked a representative from Apple’s New Product Security Division to join the meeting with ZHANG. At the conclusion of their meeting, ZHANG was asked to turn in all Apple-owned devices, and ZHANG was advised he would then be walked off the campus. ZHANG turned over to Apple two (2) Apple iPhones and one (1) MacBook laptop computer. Apple security then immediately disabled ZHANG’s remote network access, badge privileges, network access, and other employee accesses. ZHANG was also reminded about Apple’s intellectual property policy, and ZHANG acknowledged that he understood and would comply.
13. On May 1, 2018, Apple New Product Security asked that the internal Apple team overseeing the confidential Databases where Apple’s materials, including proprietary and confidential materials, are stored began reviewing ZHANG's historical network user activity. At the same time, an Apple Global Security attorney began a physical security review of ZHANG's building access and activities on the Apple campus. The Apple security attorney also requested forensic analysis of ZHANG's Apple-owned devices from Apple Information Security.

14. Apple’s database security team found that in the days just prior to April 30, 2018, ZHANG’s Apple network activity increased exponentially compared to the prior two years of his employment. The majority of his activity consisted of both bulk searches and targeted downloading copious pages of information from the various confidential database applications. The information contained within the downloading contained trade secret intellectual property, based on the level of ZHANG’s access within Apple's autonomous vehicle team.

15. Historical analysis of ZHANG’s network activity by Apple Information Security (AIS) show that with the confidential database A (the name of which is known to the affiant), ZHANG generated 581 rows of user activity on April 28, 2018 alone. On April 30, 2018, ZHANG generated 28 rows of user activity. By comparison, ZHANG generated 610 rows of user activity during the entire previous month. The amount of activity is unusual for ZHANG given that he announced his resignation on April 30, 2018.

16. AIS historical network activity of ZHANG from confidential database B (database containing technical documents for the Project) reflect 3,390 rows of user activity generated on April 28 and April 29, 2018. By comparison, ZHANG generated 1,484 rows of user activity over the time period of July 2017 through March 2018. Some of the technical .pdf documents
downloaded on April 28 and April 29, 2018 include confidential topics such as Prototypes and Prototype Requirements (power requirements, low voltage requirements, battery system, drivetrain suspension mounts, etc.) As noted above, this amount of downloading activity is unusual for ZHANG given his resignation on April 30, 2018.

17. Apple Security’s review of swipe badge access and close circuit television footage revealed that ZHANG had been on Apple’s campus at or around 9:14 p.m. on the evening of Saturday, April 28, 2018. CCTV footage showed that ZHANG entered both the autonomous vehicle software and hardware labs, and left the building less than an hour later carrying a computer keyboard, some cables, and a large box. ZHANG’s network activity, physical presence on campus, and removal of Apple property all occurred during ZHANG’s paternity leave - contrary to Apple corporate policy. ZHANG’s activity was particularly alarming to several groups within Apple’s hierarchy: the New Product Security Division, Apple’s Research and Development team overseeing the Autonomy Project, and Apple’s Global Security Investigations Group since it occurred in the few days prior to ZHANG’s resignation from Apple.

18. The Apple security attorney then contacted Apple Employee Relations on May 1, 2018, to discuss bringing ZHANG back to Apple for a follow-up interview. ZHANG was contacted and replied later in the evening of May 1, agreeing to be re-interviewed by Apple.

19. On May 2, 2018, ZHANG was interviewed a second time by the Apple security attorney and an Apple employee relations representative whose identity is known. During the interview, ZHANG admitted to pursuing employment with X-Motors while still employed at Apple. ZHANG initially denied coming onto the Apple campus during his paternity leave and denied removing items that were Apple property. As the interview progressed, Apple security
personnel confronted ZHANG verbally, stating that Apple was aware that ZHANG was, in fact, on the Apple campus during the evening of April 28, 2018. After being confronted with this information, ZHANG recanted his earlier denials and admitted to being present on the Apple campus while still on paternity leave. ZHANG further admitted to taking the online data from “the Databases” while on paternity leave. ZHANG also admitted removing items from the laboratories prior to his paternity leave (including two circuit boards and a Linux server from the hardware lab). ZHANG’s reason for these actions were that he took the hardware because he thought the hardware might benefit him in a new position within Apple. (Prior to taking paternity leave, ZHANG had begun negotiations to transfer to a separate proprietary research program at Apple, but the transfer had never taken place.) ZHANG further explained that he had compiled and downloaded the data because ZHANG has an interest in platforms and wanted to study the data on his own.

20. ZHANG admitted to being shown a proprietary chip by colleagues while on campus during the evening of Saturday, April 28, 2018. Further, ZHANG admitted “air-dropping” the data he had taken from Apple’s system onto a personally-owned device (a device not owned by Apple), which ZHANG identified as his wife’s laptop computer. ZHANG provided the Apple interviewers consent to search ZHANG’s wife’s laptop for any Apple intellectual property. ZHANG also offered to return the Linux server and circuit boards he had taken from the hardware lab.

21. ZHANG departed the Apple campus during the May 1 interview and returned in less than an hour with the computer ZHANG identified as his wife’s laptop computer (Subject Computer), along with a Linux server and the two circuit boards ZHANG had admitted to taking from Apple. The Apple security attorney and the employee relations representative performed a
cursory review of the Subject Computer in ZHANG's presence for any intellectual property and noted several folders of concern, particularly a folder entitled “RECENT” that contained approximately 40GB worth of data. Additionally, the laptop's system event logs reflected “AirDrop” activity on both April 29, 2018 and April 30, 2018.

22. Apple security personnel asked ZHANG if he further ex-filtrated or forwarded any of the data on his wife’s laptop, which ZHANG denied. ZHANG was advised that the Apple team would need to keep the Subject Computer in order to perform a more in-depth search for Apple intellectual property, to which ZHANG consented.

23. Apple security personnel has advised the FBI that at the present time, the Apple Digital Forensic Investigations team has discovered that approximately 60 percent of the data on the Subject Computer was “highly problematic;” the complete evaluation remains ongoing.

24. ZHANG was voluntarily terminated from Apple effective May 5, 2018 (though his accesses and permissions had been de-activated since April 30, 2018), and now claims to be working for XMotors out of their Mountain View, California location. ZHANG also advised the Apple investigators that he is planning to move his family to Guangzhou, China in the near future.

**FILES RECOVERED FROM SUBJECT COMPUTER**

25. Apple Information Security provided the FBI with a sample set of files Apple identified as belonging to Apple and recovered from the Subject Computer along with technical descriptions of each file. The information contained in each file is largely technical in nature, including engineering schematics, technical reference manuals, and technical reports.

26. One of these files was identified as by its specific file name (known to the affiant), and it is a 25-page pdf document containing electrical schematics for one of the circuit boards that
form Apple’s proprietary infrastructure technology for the Project. An excerpt of the schematic showing the Intellectual Property caveat is included below:

27. The file was only accessible to certain Apple employees that were disclosed on the Project as described below. This single file serves as the basis for the instant criminal charge. The Subject Computer is currently in the possession of the FBI, having been seized from Apple pursuant to a search warrant issued by U.S. Magistrate Judge Susan van Keulen on June 22, 2018.

**APPLE’S STEPS TO PROTECT ITS INTELLECTUAL PROPERTY**

28. Apple goes to great lengths to protect data and intellectual property for the Project. The Databases are protected by several layers of access control. First, an employee must be logged into Apple’s virtual private network (VPN). Accounts for VPN are provisioned during the onboarding process for new hires and controlled via an internal tool. The employee must then download an internal application and install the VPN. Next, the employee must be granted “disclosure” for the Project. Disclosure status allows an employee to receive information for the Project.
29. Apple uses an internal software tool to manage requests for project disclosure and maintains a record of all disclosures. An employee has to be "sponsored" for disclosure on the Project by someone who is already disclosed. The sponsor will submit a disclosure request on behalf of the employee through the disclosure tool. The request must include a business justification for the employee to be granted access. An administrator reviews the request and approves or denies it. Approximately 5,000 of Apple's over 135,000 full time employees are disclosed on the Project.

30. Not all employees disclosed on the Project are granted access to the Databases. After receiving disclosure, an employee must also separately request database access, unless they are designated as a "core employee" for the Project.

31. ZHANG had core employee status and access to the Databases because he was working full time on the Project under the Research and Development organization. Approximately 2,700 employees have access to one or more of the Databases.

32. Apple also goes to great lengths to communicate the importance of secrecy to its employees. Before starting at Apple, corporate employees must sign an Intellectual Property Agreement (IPA). The IPA specifies that an employee may not use Apple's intellectual property except as authorized by Apple, including a prohibition against transfer and transmission of intellectual property without Apple's consent.

33. ZHANG signed an IPA on October 28, 2015. In addition, ZHANG took an annual Business Conduct course which discussed appropriate handling of confidential material. The training explained that confidential material includes unannounced product designs and features, project or product timelines and staffing, project code names and marketing and financial information, among other things.
34. The annual Business Conduct training also explained that once an employee is formally
disclosed on a project, an employee has authorized awareness of a confidential project, can
discuss project details with people disclosed on the project, and may be given access to specific
confidential information or documents. The training stated that being disclosed does not mean an
employee can disclose other people at will.

35. Employees disclosed on the Project must also attend an in-person secrecy training for
the Project. ZHANG attended the secrecy training on December 9, 2015. The training covered
the importance of keeping the nature and the details of the Project secret and avoiding intentional
or unintentional information leaks. The training reviewed methods for ensuring information
about the project is only provided to individuals disclosed on the project, the fact that family
members should not have access to information about the Project, as well as possible
consequences for providing information or confirmation of information to non-disclosed
individuals, including employment termination. The training also covered Apple’s policy
prohibiting employees from storing IP on devices over which they do not have personal control,
and requirements for storing and transmitting Project documents using secure mechanisms.

**INTERVIEW OF ZHANG BY FBI AGENTS**

36. ZHANG was interviewed by Agents from the FBI on June 27, 2018, at the time of an
execution of a Federal search warrant at his residence. ZHANG admitted to taking files from
the Project, and further admitted to transferring these files to a non-Apple digital device,
described by ZHANG as his wife’s laptop computer (Subject Computer). ZHANG told the
Agents that because he needed to turn-in his Apple-owned laptop upon resignation, he
transferred the files to Subject Computer for access in the future.
ZHANG'S INTERNATIONAL TRAVEL PLANS

37. On July 7, 2018, FBI Agents learned that ZHANG purchased a last-minute round-trip airline ticket with no co-travelers, departing San Jose, California on July 7, 2018 traveling to Beijing, China with a final destination of Hangzhou, China aboard Hainan Airlines. Agents intercepted ZHANG at the San Jose International Airport after he had passed through the security checkpoint of Terminal B, where he was arrested by federal agents without incident based on probable cause to believe that he had committed theft of trade secrets in violation of 18 U.S.C. § 1832.

CONCLUSION

38. Through my training and experience as an FBI Agent, I believe that ZHANG used his employment as an Apple employee, working on a secretive program, to obtain intellectual property and trade secrets from Apple prior to resigning from Apple. ZHANG admitted both to Apple and to the FBI to taking Apple’s data and admitted “air-dropping” this information onto Subject Computer. Subject had received initial Intellectual Property training and annual training thereafter which would have prohibited such behavior. Further, ZHANG signed an Intellectual Property Agreement on October 28, 2015, indicating that ZHANG understood his responsibilities and would abide by Apple’s policies.

39. Based upon the foregoing, my training and experience, and the training and experience of agents and investigators involved in this investigation, I believe that there is probable cause to believe that ZHANG has committed the crime of theft of trade secrets in violation of Title 18, United States Code Section 1832.
Sworn to before me this 94th day of July, 2018

HONORABLE VIRGINIA K. DeMARCHI
United States Magistrate Judge
Case 5:18-cr-00312-EJD   Document 1   Filed 07/09/18   Page 15 of 15

DEFENDANT INFORMATION RELATIVE TO A CRIMINAL ACTION - IN U.S. DISTRICT COURT

BY: ☒ COMPLAINT ☐ INFORMATION ☐ INDICTMENT ☐ SUPERSEDING

OFFENSE CHARGED

Count One: 18 U.S.C. § 1832(a)(1) – Theft of Trade Secrets

☐ Petty
☐ Minor
☐ Misdemeanor

☒ Felony

PENALTY: 10 years imprisonment, $250,000 fine, $100 special assessment, 3 years' supervised release

Name of District Court, and/or Judge/Magistrate Location
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

DEFE  

XIAOLANG ZHANG

DISTRICT COURT NUMBER

MAG

CR 18 70919

PROCCEEDING

Name of Complaintant Agency, or Person (& Title, if any)
Eric M. Proudfoot, FBI

☐ person is awaiting trial in another Federal or State Court, give name of court

☐ this person/proceeding is transferred from another district per (circle one) FRCrP 20, 21, or 40. Show District

☐ this is a reprosecution of charges previously dismissed which were dismissed on motion of:

☐ U.S. ATTORNEY ☐ DEFENSE

SHOW DOCKET NO.

☐ this prosecution relates to a pending case involving this same defendant prior proceedings or appearance(s) before U.S. Magistrate regarding this defendant were recorded under

MAGISTRATE CASE NO.

Name and Office of Person Furnishing Information on this form
ALEX G. TSE, Acting U.S. Attorney

☐ U.S. Attorney ☐ Other U.S. Agency

Name of Assistant U.S. Attorney (if assigned)
Amie D. Rooney

ADDITI  

ONAL INFORMATION OR COMMENTS

PROCESS:

☐ SUMMONS ☒ NO PROCESS* ☐ WARRANT

If Summons, complete following:
☐ Arraignment ☐ Initial Appearance

Defendant Address:

Comments:

Bail Amount: ___________

* Where defendant previously apprehended on complaint, no new summons or warrant needed, since Magistrate has scheduled arraignment

DATE OF ARREST
July 7, 2018

DATE TRANSFERRED TO U.S. CUSTODY

☐ This report amends AO 257 previously submitted

DATE/TIME: _______________ Before Judge:

FILING

FILED

JUL 09 2018

CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE

IS NOT IN CUSTODY

Has not been arrested, pending outcome this proceeding.

1) ☐ If not detained give date any prior summons was served on above charges

2) ☐ Is a Fugitive

3) ☐ Is on Bail or Release from (show District)

IS IN CUSTODY

☐ On this charge

4) ☒ On another conviction

☐ Federal ☐ State

5) ☒ Awaiting trial on other charges

If answer to (6) is "Yes", show name of institution

6) ☐ And has detainer been filed?

☐ Yes ☐ No

If "Yes" give date filed

Or... if Arresting Agency & Warrant were not

DATE TRANSFERRED TO U.S. CUSTODY _______________
COMPLAINT

UNITED STATES OF AMERICA

- v. -

JIAQIANG XU,

Defendant.

SOUTHERN DISTRICT OF NEW YORK, ss.: JOSEPH M. ALTIMARI, being duly sworn, deposes and says that he is a Special Agent with the Federal Bureau of Investigation ("FBI"), and charges as follows:

COUNT ONE

1. From in or about November 2014, through on or about December 7, 2015, in the Southern District of New York and elsewhere, JIAQIANG XU, the defendant, with intent to convert a trade secret that is related to a product and service used in and intended for use in interstate and foreign commerce, to the economic benefit of others than the owner thereof, and intending and knowing that the offense would injure the owner of that trade secret, knowingly did steal, and without authorization appropriate, take, carry away, and conceal, and by fraud, artifice and deception obtain such information; and without authorization did copy, duplicate, sketch, draw, photograph, download, upload, alter, destroy, photocopy, replicate, transmit, deliver, send, mail, communicate, and convey such information; and attempted to do so, to wit, XU stole and converted to his own use the source code for a piece of proprietary software, which source code was a trade secret of a company for which XU previously worked.

(Title 18, United States Code, Section 1832.)

The bases for my knowledge and for the foregoing charges are, in part, as follows:

2. I am a Special Agent with the FBI. I am currently assigned to the FBI's White Plains Resident Agency, where I investigate a variety of crimes related to counter-intelligence, including espionage and the theft of trade secrets. I have participated in an investigation of the
theft of trade secrets, as set forth below. I am familiar with the facts and circumstances set forth below from my personal participation in the investigation, including my review of pertinent documents, and from my conversations with others, including other Special Agents with the FBI, and representatives of a particular U.S. company (the “Victim Company”) with expertise regarding the relevant software (the “Proprietary Software”) and its source code. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

The Proprietary Software

3. Based on my review of FBI reports, information provided by the Victim Company, publicly available information, and my participation in this investigation, I have learned the following about the Proprietary Software: the Proprietary Software is a clustered file system developed and marketed by the Victim Company in the United States and other countries. A clustered file system facilitates faster computer performance by coordinating work among multiple servers. The Victim Company produces the Proprietary Software for use in high-performance computer systems. Customers include government agencies and private corporations.

4. According to open source information, the Proprietary Software is a key component of some of the world’s largest scientific supercomputers, as well as commercial applications requiring rapid access to large volumes of data. Industries that use the Proprietary Software include digital media, engineering, design, business intelligence, financial analytics, seismic data processing, geographic information systems, and scalable file serving.

5. According to a representative of the Victim Company, the source code underlying the Proprietary Software (the “Proprietary Source Code”)—that is, the computer instructions and commands that can be compiled or assembled into the Proprietary Software—is itself proprietary information, which the Victim Company does not sell or otherwise make available to customers.

6. According further to a representative of the Victim Company, the Victim Company takes significant precautions to protect the Proprietary Source Code as a trade secret. Among other things, the Proprietary Source Code is stored behind a company firewall and can only be accessed by a small subset of the Victim Company’s employees. Before receiving Proprietary Source Code access, Victim Company employees must first request and receive approval from a particular Victim Company official. Victim Company employees must also agree in writing at both the outset and the conclusion of their employment that they will maintain the confidentiality of any proprietary information. The Victim Company takes these and other precautions in part because the Proprietary Software and the Proprietary Source Code are economically valuable, which value depends in part on the Proprietary Source Code’s secrecy. The Victim Company invests millions of dollars in the Proprietary Software each year for research and development, and the Proprietary Software generates tens of millions of dollars in revenue each year for the Victim Company.
The Defendant

7. From my review of FBI reports and information obtained from the Victim Company, I have learned the following:

a. JIAQIANG XU, the defendant, worked for a branch of the Victim Company in China (the “China Branch”) from November 2010 to May 2014.

b. At the China Branch, XU worked as a software engineer and had full access to the Proprietary Source Code, including the ability to download the Proprietary Source Code to a computer or digital storage device.

c. On or about November 30, 2010, XU signed a four-page document entitled “Agreement Regarding Confidential Information and Intellectual Property” (the “Confidentiality Agreement”). By signing the Confidentiality Agreement, XU agreed that he would not, among other things, disclose “any confidential information or material of [the Victim Company] or its affiliates.” The Confidentiality Agreement specified that “Confidential information . . . shall include but [is] not limited to any information or material . . . generated or collected by or utilized in the operations of [the Victim Company] or its affiliates . . . which has not been made available generally to the public.”

d. In May 2014, XU voluntarily resigned from the Victim Company.

The Investigation

8. In 2014, the FBI received a report that an individual in China—who, as described below, was later identified as JIAQIANG XU, the defendant—claimed to have access to the Proprietary Source Code and to be using the Proprietary Source Code in business ventures that were not related to the Victim Company’s clients. Other Special Agents and I thereafter conducted an investigation, which included the use of undercover law enforcement officers (“UC-1” and “UC-2,” and collectively “the UCs”).

9. In or around November 2014, UC-1 contacted JIAQIANG XU, the defendant, via email. For purposes of this investigation, UC-1 posed as a financial investor aiming to start a large-data storage technology company (the “UC Company”). I have reviewed copies of emails that UC-1 exchanged with XU between November 2014 and February 2015. From my review of those emails, I have learned the following:

a. On or about November 27, 2014, UC-1 wrote to XU, among other things: “I am currently investing in and working with a new technology company which is seeking to develop improved and more secure data storage systems. As you may be aware, there is exciting new development in this area and the opportunities to be involved with cutting edge start up companies are excellent.”

b. On or about November 27, 2014, XU responded, among other things: “Nice to hear from you. I am very interested in opportunities working over the architecture
design and code development for cutting edge storage systems. I have several years working experience over this field and spent most of my career in [the Victim Company] working on the development of [the Proprietary Software] which is a largescale parallel storage system used in lots of hyperscale cluster systems in the world. I am looking forward to discuss with you on the project and further opportunities. Thank you very much! Best Regards, Jiaqiang Xu.”

c. On or about February 19, 2015, XU emailed to UC-1 a copy of XU’s resume (the “Xu Resume”). According to the Xu Resume, XU lived in Beijing, China; his skills included “Operating Systems and Parallel File System”; he had received a master of science degree in computer science from a university in the United States; he had worked at the Victim Company from November 2010 through June 2014 (“Job Role: Research & Development of [the Proprietary Software]”); and he thereafter worked at another company as “Architect of the Storage Platform for Cloud Computing”.

10. I have reviewed additional emails between JIAQIANG XU, the defendant, and the UCs, from in or about March 2015, by which date UC-2 had been brought into the email chain by UC-1. For purposes of this investigation, UC-2 was posing as a project manager, working for UC-1. From my review of those emails, I have learned that on or about March 16, 2015, XU sent an email to UC-1 and UC-2 (“the Source Code Email”). In the Source Code Email, XU described some of his past experience with the Proprietary Software and reported that he had “attached some sample code of [his] previous work in [the Victim Company].” XU also pasted a “short [Proprietary Software]+NFS related patch” directly into the Source Code Email, purportedly for the purpose of showing XU’s “coding style.”

11. After receiving the Source Code Email, other Special Agents and I showed the computer code in it to a representative of the Victim Company (“Employee-1”), who has expertise in the Proprietary Software. Employee-1 confirmed that the Source Code Email included proprietary Victim Company material that related to the Proprietary Source Code.

12. On or about April 12, 2015, JIAQIANG XU, the defendant, and UC-2 participated in a recorded audio conversation using a commercial communication service (the “Communication Service”), which had been arranged via emails between XU and the UCs. I have reviewed that recording, as well as a draft transcript of that conversation, which was conducted in English. From my review of those materials, I have learned of the following conversation, in substance and in part:

a. XU stated that “[the Proprietary Software] is not open source,” to which UC-2 responded “No I know it isn’t.”

b. UC-2 inquired as to whether XU “was allowed to have this code, since it’s [the Victim Company]’s” and clarified that UC-2 was asking if UC-2 should “be a little . . .

1 Based on my training and experience, I know that the Communication Service allows for, among other things, remote voice communication.

2 Based on my training and experience, I know that the term “open-source software” refers to software whose source code is made publicly available.
discreet as to who [UC-2] show[ed] it to.” XU replied that “Yes, we signed some, you know, signed some files there but actually I can, um, I can, I have all the code.”

c. UC-2 asked, “Oh you do have all the code?” XU replied, “Yeah I have all the [Proprietary Software] code.”

d. UC-2 later said, “I just want to assure you that like, if you started working with us, not only will we pay you for your services but if you brought some of this code, [UC-1 would] be more than willing to pay you for that as well. . . . You, you’ll be fully compensated for anything that you can offer to us. . . . [A]t the end of the day, the most important thing is, is we just want a good product and that is going to satisfy our needs.”

e. XU replied, among other things, that in his experience, start-up companies often used code obtained from large, established companies, “because no one, ah, no one want to, you know, code from the, the first line.” Based on my training, experience, and participation in this investigation, I believe that XU was intimating to UC-2 that XU could provide the Proprietary Source Code to UC-2 to accelerate the development of UC-2’s company’s product.

f. XU reported that he had already used a portion of the Proprietary Source Code as part of his then-current employment at a technology startup company.

13. On or about May 11, 2015, JIAQIANG XLI, the defendant, and UC-2 had another recorded audio conversation using the Communication Service. I have reviewed that recording, as well as a draft transcript of that conversation, which was conducted in English. From my review of those materials, I have learned that XU said the following, in substance and in part:

a. XU again stated that he had used “some of the [Proprietary Software] code” in his work after he left the Victim Company.

b. XU stated that he was willing to consider providing UC-2’s company with the Proprietary Source Code as a platform for UC-2’s company to facilitate the development of UC-2’s company’s own data storage system.

c. XU informed UC-2 that if UC-2 set up several computers as a small network, then XU would remotely install the Proprietary Software so that the UC’s could test it and confirm its functionality.  

3 Based on my training, experience, and participation in this investigation, I believe that XU’s reference to having “signed some files” was an acknowledgement that he had signed the Confidentiality Agreement as part of his employment at the Victim Company, see supra 6. 7(c). In addition to the Confidentiality Agreement, XU may also have been referring to an exit affidavit that he completed before leaving the Victim Company’s employment. I have reviewed a Victim Company document with the header “Affidavit,” which appears to have been completed by XU in Mandarin — which I do not speak — in connection with the conclusion of XU’s employment by the Victim Company. Among other things, that document bears XU’s identification card number. It also reads, in part, in English “I hereby represent that I have settled/returned or will settle/return all debit/assets due [the Victim Company].”
14. I have reviewed additional emails exchanged between JIAQIANG XU, the defendant, and UC-2 in or about early June 2015. On or about June 1, 2015, UC-2 emailed XU to confirm that the UCs would set up several computers per XU’s specifications. On or about June 2, 2015, XU responded, thanked UC-2, and stated, among other things, that he “ha[d] a lot of thinking about what we can do in storage layer to better support the big-data applications.”

15. In or around early August 2015, I and other FBI agents arranged for a computer network to be set up, consistent with the specifications that JIAQIANG XU, the defendant, had provided (the “UC Network”).

16. On or about August 6, 2015, JIAQIANG XU, the defendant, and UC-2 had another recorded audio conversation using the Communication Service. I have reviewed that recording, as well as a draft transcript of that conversation, which was conducted in English. From my review of those materials, I have learned the following, in substance and in part:

a. UC-2 confirmed to XU that UC-2 had set up the network that XU had requested and provided XU with instructions for how to access that network.

b. XU stated that “I will have a try and ah try to install it [i.e., the Proprietary Software]. And ah, I think, ah, it will be good.”

17. Based on my conversations with other law enforcement officers and my review of the UC Network’s contents, I have learned that in or around early August 2015, files were remotely uploaded to the UC Network (the “Xu Upload”). Thereafter, on or about August 26, 2015, XU and UC-2 exchanged emails confirming that UC-2 had received the Xu Upload.

18. On or about September 21, 2015, I made a digital copy of the Xu Upload available to a Victim Company employee who has expertise regarding the Proprietary Software and the Proprietary Source Code (“Employee-2”) for Employee-2 to review. Based on my discussions with Employee-2, I have learned the following:

a. Based on Employee-2’s assessment of the Xu Upload, the Xu Upload appeared to contain a functioning copy of the Proprietary Software.

b. The Xu Upload did not appear to be the official Proprietary Software package that the Victim Company provides to licensed customers. Among other irregularities, the Xu Upload appeared to have been built by a “build host” (that is, a computer system) that was not on the Victim Company’s network. Additionally, the Xu Upload’s version of the Proprietary Software had a “build date” that was inconsistent with the date on which the Victim Company’s

---

4 Based on my training, experience, and conversations with Victim Company employees, I know that source code cannot be completely reverse engineered from software. In other words, it does not appear that XU was agreeing to provide the Proprietary Source Code to the UCs but instead to demonstrate to them that XU himself had access to the Proprietary Source Code and could use it to build the UCs a working version of the Proprietary Software.
developers had created the licensed edition of that same version of the Proprietary Software.

c. Notwithstanding the irregularities noted in the preceding paragraph, the Xu Upload’s version of the Proprietary Software appeared to have been built using coding practices used by the Victim Company’s developers for internal development purposes.

d. Based on the foregoing, among other factors, it appeared to Employee-2 that the Xu Upload had been built by someone with access to the Proprietary Source Code who was not working within the Victim Company or otherwise at the Victim Company’s direction.

19. On or about the morning of December 7, 2015, JIAQIANG XU, the defendant, met with UC-2 at a hotel in White Plains, New York (the “Hotel”). I have listened to a recording of that meeting. Based on my review of that recording and my conversations with UC-2, I have learned that during the meeting, XU said the following in substance and in part:

a. XU has used the Proprietary Source Code to make software to sell to customers.

b. XU knew the Proprietary Source Code to be the product of two decades’ work on the part of Victim Company engineers.

c. XU had used the Proprietary Source Code to build a copy of the Proprietary Software, which XU had uploaded and installed on the UC Network (i.e., the Xu Upload).

d. XU knew that the copy of the Proprietary Software that XU had installed on the UC Network contained information identifying the Proprietary Software as the Victim Company’s property, which could reveal the fact that the Proprietary Software had been built with the Proprietary Source Code without the Victim Company’s authorization. XU indicated to UC-2 that XU could take steps to prevent detection of the Proprietary Software’s origins—i.e., that it had been built with stolen Proprietary Source Code—including writing computer scripts that would modify the Proprietary Source Code to conceal its origins.

e. UC-2 and XU arranged to meet again in the afternoon.

20. On or about the afternoon of December 7, 2015, UC-2 and JIAQIANG XU, the defendant, again met, along with UC-1, in the Hotel. I watched and listened to portions of that meeting which was transmitted live to monitoring agents, and audio and video recorded. Based on my monitoring of the meeting as well as my conversations with the UCs, I have learned that the following occurred during that meeting, in substance and in part:

a. XU showed UC-2 a copy of what XU represented to be the Proprietary Source Code on XU’s laptop. XU noted to UC-2 a portion of that code which indicated that it originated with the Victim Company as well as the date on which it had been copyrighted.

b. XU reiterated to the UCs that he knew the Proprietary Source Code had been the product of extended work on the part of Victim Company employees, which continued to the present day.
c. XU stated that XU had previously modified the Proprietary Source Code's command interface to conceal the fact that the Proprietary Source Code originated with the Victim Company.

d. XU identified multiple specific customers to whom XU had previously provided the Proprietary Software using XU's stolen copy of the Proprietary Source Code. XU acknowledged that the Proprietary Source Code had considerable value.

WHEREFORE, deponent respectfully requests that JIAQIANG XU, the defendant, be imprisoned, or bailed, as the case may be.

[Signature]

JOSEPH M. ALTIMARI
Special Agent
Federal Bureau of Investigation

Sworn to before me this 8th day of December 2015

[Signature]

HONORABLE JUDITH C. McCArTHY
United States Magistrate Judge
Southern District of New York
IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Holding a Criminal Term

Grand Jury Sworn in on November 3, 2016

UNITED STATES OF AMERICA : CRIMINAL NO. 17-110 (CRC)

v.

VIOLATIONS:

SHAN SHI, : 18 U.S.C. § 1832
KUI BO, : (Theft of Trade Secrets)
GANG LIU, : 18 U.S.C. § 1831 (Economic Espionage)
SAMUEL OGOE, : 18 U.S.C. § 1956(h) (Conspiracy to Launder Monetary instruments)
UKA UCHE, : FORFEITURE:
HUI HUANG, : 18 U.S.C. §§ 981(a)(1); 982; & 2323; &
TAIZHOU CBM FUTURE NEW MATERIAL SCIENCE AND TECHNOLOGY CO. LTD, AND : 21 U.S.C. § 853(p); 28 U.S.C. § 2461(c)
CBM INTERNATIONAL, INC. :

Defendants.

INDICTMENT

The Grand Jury charges that:

INTRODUCTORY ALLEGATIONS

At all times material to this Indictment:
DEFENDANTS AND OTHER ENTITIES

1. The Ministry of Industry and Information Technology (“MIIT”) is an agency of the People’s Republic of China (“PRC”), tasked in part to help develop the PRC as a marine power. The PRC State Council created MIIT in March 2008 to assume the functions of several previous ministries and offices. MIIT has a significant role in regulating major industries and approving new industrial investments and projects in key areas such as information technology, telecommunications, and national defense.

2. The Commission of Science, Technology, and Industry for National Defense (“COSTIND”) is administered by the PRC through MIIT. COSTIND initiated the Key Laboratory of Science and Technology for National Defense program (“KLSTND”). COSTIND administers Harbin Engineering University (“HEU”), and the China Shipbuilding Industry Corporation (“CSIC”).

3. HEU is a China-based entity that has extensive ties to the Chinese People’s Liberation Army (“PLA”) and Navy.

4. CSIC develops, produces, and repairs military and commercial vessels, and related products.

5. China National Offshore Oil Company (“CNOOC”) is responsible for offshore oil and gas exploration and exploitation in China.

6. Linhai City is a City within Taizhou City, which is within Zhejiang Province, China.
7. Defendant Taizhou CBM-Future New Material Science and Technology Co. Ltd. (“CBMF”) is a China-based company.

8. Defendant SHI is a naturalized U.S. citizen who resides in Houston, Texas, and had ties to Houston-based oil firms, as described below. SHI is a graduate of HEU. SHI has previously worked at the forerunner of CSIC where he was involved with the design of at least one PLA Navy ship. In a resume current as of March 2016, SHI indicated that he was then-employed as an overseas professor at HEU, and as a senior technical advisor at CSIC.

9. CBM International, Inc. (“CBMI”) was established in March 2014, in Houston, with CBMF as its only shareholder. The shareholders of CBMI were PRC-Person 1, a person known to the grand jury, who was the president of CBMF and provided funding for CBMI’s operations; PRC-Person 2, a person known to the grand jury; and SHI, who, based in Houston, became President of CBMI.

10. Kui BO is a Canadian citizen with a U.S. visa who has recently applied for U.S. Legal Permanent Resident status. BO resides in the Dallas, Texas area. BO was an employee of CBMI. At CBMI, BO was involved in day-to-day operations.

11. Samuel OGOE was born in Ghana and is a naturalized U.S. citizen. OGOE was employed at CBMI until late 2015, when he became a contract employee. Previously, OGOE was employed by a company (“Company A”) as a Materials Development Manager where he had access to Company A proprietary and trade secret data beginning in or about 2008.
12. U.S. Person 1, who was a defendant in a previous indictment, is a U.S. citizen who was employed as a Production Supervisor by Company A in Houston where he had access to Company A proprietary and trade secret data beginning in or about 2007.

13. Uka UCHE was born in Nigeria and is a naturalized U.S. citizen. UCHE was employed by Company A in Houston where he worked as an Operations Systems Specialist and had access to Company A proprietary and trade secret data beginning in or about 2008.

14. Gang LIU is a Chinese citizen who had been present in the United States on a student visa since 2008. As of February 2017, LIU was a U.S. permanent resident alien. LIU previously worked for Company A as a Material Development Engineer and had access to proprietary and trade secret data beginning in or about 2013. LIU was highly involved in the research and development (“R&D”) at CBMF and CBMI.

15. Hui HUANG is a Chinese national who lives in China. HUANG is an employee of CBMF and is involved in many of the interactions and taskings to CBMI employees. HUANG has traveled to the United States on numerous occasions during his employment with CBMF.

THE PRC’s GOAL OF BECOMING A MARINE POWER

16. The PRC sets out a series of military, social and economic development initiatives known as “Five-Year Plans” (“Plans”) to map out goals and guidelines for Chinese economic development in various economic sectors for the following five-year period. Recent Plans have included mandates for the development of the PRC’s marine industry. For example, the Twelfth Five-Year Plan, governing 2011 to 2015, directed the PRC to expand marine engineering equipment manufacturing, strengthen the R&D of critical marine technologies, and carry out trials
of marine development in provinces including Zhejiang Province, which is just west of the East China Sea. As part of the PRC’s Thirteenth Five-Year Plan, governing 2016-2020, the PRC publicly declared its desire to become a strong maritime country as a national priority. MIIT sought to promote the research and development of China’s marine equipment industry and realize the country’s goal of becoming a “marine power” in the world. The PRC government tasked its government ministries like MIIT, its state-owned enterprises (“SOE”s) and its territories to further these goals and guidelines.

17. As part of the Twelfth Five-Year Plan, the PRC’s MIIT coordinated many of the efforts to make the PRC a marine power, including prioritizing the development of engineered components of deepwater buoyancy materials for water depth ranging from 1,500-3,000 meters below sea level. MIIT provided funds to Zhejiang Province in order that Zhejiang Province, which includes Taizhou City, where CBMF is located, which includes the smaller division of Linhai City, could further develop this goal.

18. As demonstrated below, CBMF was tasked pursuant to the PRC’s Twelfth Five-Year Plan to develop the PRC’s marine engineering equipment manufacturing capability, including the underwater equipment referenced above, for the benefit of the PRC. In furtherance of this PRC goal, CBMF stole the trade secrets of Company A, whose true name is substituted in this indictment for purposes of confidentiality, in order to create a manufacturing facility in China for the marine industry product known as syntactic foam.

19. Syntactic foam consists of tiny hollow spheres suspended in an epoxy resin. The combination of hollow spheres encased in epoxy creates a strong, light material ideal for a variety of applications. Strength and other performance characteristics can be improved by chemical
surface treatment of the spheres. Syntactic foam may be tailored for both commercial (including drill riser buoyancy modules (“DRBM”) in oil exploration) and military use (including aerospace, underwater, and stealth technology). Syntactic foam could include only microspheres, commonly measured in microns, or be a composite of microspheres and slightly larger macrospheres (typically having diameters from 4 millimeters to 40 millimeters).

**CBMF’S RELATIONSHIP TO THE PRC AND PRC SOES**

20. CBMF was part of a “National Team of Marine Engineering” and a collaborative innovation center with PRC-government entities, including SOEs HEU, CSIC, and CNOOC.

21. The purpose of the National Team of Marine Engineering was to carry out joint ventures in developing deep-sea buoyancy material, military insulation material, and new lightweight composite design to advance PRC military and civilian interests.

22. CBMF was closely tied to HEU in personnel, projects, and money: CBMF further described itself as “taking advantage of HEU’s technical resources through science and technology cooperation with military industry.” In 2015, CBMF reported it received more than half of its research funds from state funding, and that its R&D team consisted almost entirely of individuals from HEU, which also included Shan SHI.

23. In 2013 and 2014, CBMF entered into numerous contracts with HEU and CSIC to provide the above-referenced buoyancy materials.

**THE ESTABLISHMENT OF CBMI TO DEVELOP SYNTACTIC FOAM**

24. CBMF’s efforts on developing a PRC-based manufacturing plant for syntactic foam led to the development of its subsidiary, CBMI. SHI, the President of CBMI, recognized the value of Houston as a potential source for the development of syntactic foam.
25. Company A was a multinational engineering firm whose business included the development of syntactic foam. Company A’s corporate headquarters are in Sweden and it operates a subsidiary in Houston. Company A developed, sold and shipped, and intended to develop, sell and ship, syntactic foam in interstate and foreign commerce.

26. The technology for creating syntactic foam was closely held by the dominant producers and sellers of syntactic foam, including Company A, which developed advancements in the technology through intensive and costly R&D over many years. Company A is one of the four leading companies in the global syntactic foam market.

27. The PRC, seeking to further develop the technology for the reasons described above, provided funding to CBMF. Aware of the PRC’s national priority, and in order to bypass the technical, expensive, and time-consuming R&D required to develop syntactic foam themselves, the individuals named in this Indictment acquired Company A’s trade secrets relating to syntactic foam, without the authorization of Company A. SHI, LIU, and other entities known to the grand jury stole these trade secrets to benefit the PRC’s SOEs HEU, CNOOC, CSIC, and Linhai City.

28. By 2016, in line with the PRC’s goals, CBMF had a syntactic foam factory in Taizhou, and was bidding for significant contracts with a product built from the labors of Company A.

**RELEVANT STATUTES**

**The Economic Espionage Act**

Money Laundering


COMPANY A TOOK STEPS TO PROTECT ITS TRADE SECRETS

31. Company A has refined its syntactic foam design and development process over time. The production of the spheres for syntactic foam is a complex manufacturing process and Company A has continually improved its process over the past fifty years since its invention. Through its technical expertise, experience, and continued R&D investment, Company A has developed a process that afforded it a competitive advantage in the marketplace.

32. Company A’s syntactic foam technology included, but was not limited to, the following trade secrets, each of which, if stolen by a competitor could give that competitor an unfair advantage:

A. **Trade Secret 1**: Sphere Diameter Pressure and Density. Company A’s technical innovation team worked on different formulations of resin for different spheres, including the performance of each formula at different depths and densities and the results of an experimental formula developed by Company A. Company A began experimenting with the new formula in 2013 or 2014. The new formula was used by Company A to increase strength while lowering the cost of producing the spheres.

B. **Trade Secret 2**: Density Calculations. The density of different 10mm macrospheres, including the performance of specific spheres pulled from a specific batch, was a Company A trade secret. Company A tested
spheres for diameter and weight, with the results averaged to represent the entire batch. Company A density calculations would provide a competitor key information about the performance of a certain batch of Company A’s macrospheres, and benchmarks to meet in the production of the competitor’s macrospheres. Access to such density calculations at Company A was password protected and restricted to a small number of Company A employees.

C. **Trade Secret 3:** Standard Operating Procedures (“SOP”) for Hydrostatic Pressure Testing. Company A’s SOP for hydrostatic testing, which is a necessary quality control measure prior to selling the syntactic foam product to customers was a trade secret.

D. **Trade Secret 4:** Manufacturing Process Data Models. Information developed by Company A regarding the number of coats on spheres and the performance of these spheres at certain densities was a Company A trade secret. Access to the models at Company A was password protected and restricted to a small number of Company A employees.

E. **Trade Secret 5:** Theoretically Calculated Syntactic Foam Formulation. A list of raw materials and various weights associated with those materials, which could be used to make syntactic foam, was a Company A trade secret. Access to this formulation at Company A was
password protected and restricted to a small number of Company A employees.

F. **Trade Secret 6**: Macrosphere Rating & Cost. The costs for a newly developed formula related to syntactic foam was a Company A trade secret. Access to the macrosphere rating and cost information at Company A was password protected and restricted to a small number of Company A employees.

G. **Trade Secret 7**: Raw Material Prices. The prices Company A paid for various raw materials at certain volumes in 2014 was a Company A trade secret. These prices were negotiated by Company A with its suppliers. Access to raw materials pricing at Company A was password protected and restricted to a small number of Company A employees.

33. The trade secrets listed above were considered such by Company A and were protected by Company A as confidential and proprietary information. Company A used a number of reasonable measures to protect its trade secrets and its confidential proprietary information, including, but not limited to:

A. Limiting visitor access to its facilities;
B. Requiring visitors to facilities to sign a confidentiality agreement;
C. Limiting its computer network to designated employees;
D. Limiting access to the network depending on work assignations;
E. Requiring that approval for “limited access” folders may only be granted by an information technology administrator;
F. Mandating that new hires receive and sign non-competition agreements and training regarding the protection of Company A trade secrets; and

G. Requiring employees to execute non-competition agreements upon termination that included language not to divulge certain protected information, including Company A trade secrets.

**COUNT ONE**

*(Conspiracy to Steal and Convert a Trade Secret)*

34. The allegations in Paragraphs 1 through 33 of this Indictment are incorporated and re-alleged by reference herein.

35. Beginning on a date unknown to the Grand Jury but at least by, in or about March 2012, and continuing until on or about May 23, 2017, in the District of Columbia, and elsewhere, the defendants, SHI, HUANG, BO, LIU, OGOE, UCHE, CBMF, and CBMI and others known to the grand jury did knowingly and willfully combine, conspire, confederate, and agree with each other, and others known and unknown to the Grand Jury, to commit the following offenses:

A. With intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate and foreign commerce, to the economic benefit of anyone other than the owner of the trade secret, and intending and knowing that the offense will, injure any owner of that trade secret, knowingly steal, and without authorization appropriate, take, carry away, and conceal, and by fraud, artifice, and deception obtain such
information, in violation of Title 18, United States Code, Section 1832(a)(1);

B. With intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate and foreign commerce, to the economic benefit of anyone other than the owner of the trade secret, and intending and knowing that the offense will, injure any owner of that trade secret, knowingly, and without authorization copy, duplicate, sketch, draw, photograph, download, upload, alter, destroy, photocopy, replicate, transmit, deliver, send, mail, communicate, and convey such information, in violation of Title 18, United States Code, Section 1832(a)(2); and

C. With intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate and foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending and knowing that the offense will, injure any owner of that trade secret, knowingly receive, buy, and possess such information, knowing the same to have been stolen and appropriated, obtained, and converted without authorization, in violation of Title 18, United States Code, Section 1832(a)(3).
OBJECTS OF THE CONSPIRACY

36. The objects of the conspiracy were:

A. To appropriate trade secrets belonging to Company A for the benefit of another other than Company A, knowing such appropriation would injure Company A;
B. To replicate trade secrets belonging to Company A for the benefit of another other than Company A, knowing such replication would injure Company A;
C. To receive and possess trade secrets belonging to Company A for the benefit of another other than Company A, knowing such receipt and possession would injure Company A.

WAYS, MANNER AND MEANS OF THE CONSPIRACY

37. Defendants SHI, BO, LIU, OGOE, UCHE, HUANG, CBMF, and CBMI, and others both known and unknown to the grand jury, would and did carry out the conspiracy and effect its unlawful objects, that is, the stealing, appropriation, taking, carrying away, and concealing, and by fraud, artifice and deception; the copying, duplication, photographing, downloading, uploading, altering, photocopying, replicating, transmitting, delivering, sending, mailing, communicating, and conveying; and receiving, buying, and possessing the trade secrets owned by Company A, through the following manner and means, among others:

A. It was part of the conspiracy that members of the conspiracy, both known
and unknown to the grand jury, created CBMI in the United States in order to
develop CBMF’s syntactic foam manufacturing ability in China.

B. It was part of the conspiracy that members of the conspiracy, both known
and unknown to the grand jury, targeted current and former Company A employees
for hiring for the purpose of advancing CBMF’s capability to manufacture syntactic
foam.

C. It was part of the conspiracy that members of the conspiracy, both known
and unknown to the grand jury, planned to steal the confidential and proprietary
information of Company A, including its trade secrets, by accessing information
taken by current and former Company A employees.

D. It was further part of the conspiracy that members of the conspiracy, both
known and unknown to the grand jury, would acquire Company A trade secrets and
use them to promote CBMF and CBMI’s own syntactic foam and sphere
capabilities.

E. It was further part of the conspiracy that members of the conspiracy, both
known and unknown to the grand jury, arranged for the transfer of approximately
$3.1 million from CBMF to CBMI to maintain CBMI’s operations and pay CBMI’s
employee salaries.

F. It was further part of the conspiracy that Defendants SHI, BO, LIU, OGOE,
HUANG, CBMF, CBMI, and others both known and unknown to the grand jury,
understood that OGOE and LIU had executed severance agreements with Company
A in which OGOE and LIU had acknowledged the importance of proprietary
information to Company A and agreed not to share any trade secrets of Company A.

G. It was further part of the conspiracy that SHI and others both known and unknown to the grand jury coordinated the development and manufacture of syntactic foam in order to benefit PRC’s SOEs, including HEU, CNOOC, and CSIC, and Linhai City, by providing the technology and materials necessary to fulfill the PRC’s goals.

**OVERT ACTS**

38. In furtherance of the conspiracy, and to achieve the objects and purposes thereof, the Defendants SHI, BO, LIU, OGOE, UCHE, HUANG, CBMF, CBMI, and others both known and unknown to the grand jury, committed and caused to be committed the following overt acts, among others, in the District of Columbia and elsewhere:

A. Beginning on June 27, 2014, and continuing through at least May 15, 2017, employees of CBMF sent Houston-based CBMI approximately 34 wire transfers totaling approximately $3.1 million dollars. CBMF sent these wire transfers from its account at the Bank of China to CBMI’s U.S.-based account at Bank of America, ending in 6528, as follows:

<table>
<thead>
<tr>
<th>Transaction Date</th>
<th>Wired From</th>
<th>Wired To</th>
<th>Wire Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>6/27/2014</td>
<td>CBMF, China</td>
<td>CBMI, U.S.</td>
<td>$20,000.00</td>
</tr>
<tr>
<td>8/12/2014</td>
<td>CBMF, China</td>
<td>CBMI, U.S.</td>
<td>$120,000.00</td>
</tr>
<tr>
<td>9/23/2014</td>
<td>CBMF, China</td>
<td>CBMI, U.S.</td>
<td>$20,000.00</td>
</tr>
<tr>
<td>1/29/2015</td>
<td>CBMF, China</td>
<td>CBMI, U.S.</td>
<td>$100,000.00</td>
</tr>
<tr>
<td>4/1/2015</td>
<td>CBMF, China</td>
<td>CBMI, U.S.</td>
<td>$200,000.00</td>
</tr>
<tr>
<td>4/30/2015</td>
<td>CBMF, China</td>
<td>CBMI, U.S.</td>
<td>$150,000.00</td>
</tr>
</tbody>
</table>
Transfer of Specific Trade Secrets

B. On January 13, 2015, U.S. Person 1, an unindicted-coconspirator previously

<table>
<thead>
<tr>
<th>Date</th>
<th>Source</th>
<th>Destination</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>6/26/2015</td>
<td>CBMF, China</td>
<td>CBMI, U.S.</td>
<td>$60,000.00</td>
</tr>
<tr>
<td>7/20/2015</td>
<td>CBMF, China</td>
<td>CBMI, U.S.</td>
<td>$30,000.00</td>
</tr>
<tr>
<td>7/23/2015</td>
<td>CBMF, China</td>
<td>CBMI, U.S.</td>
<td>$170,000.00</td>
</tr>
<tr>
<td>9/14/2015</td>
<td>CBMF, China</td>
<td>CBMI, U.S.</td>
<td>$130,000.00</td>
</tr>
<tr>
<td>9/30/2015</td>
<td>CBMF, China</td>
<td>CBMI, U.S.</td>
<td>$70,000.00</td>
</tr>
<tr>
<td>11/4/2015</td>
<td>CBMF, China</td>
<td>CBMI, U.S.</td>
<td>$50,000.00</td>
</tr>
<tr>
<td>11/18/2015</td>
<td>CBMF, China</td>
<td>CBMI, U.S.</td>
<td>$150,000.00</td>
</tr>
<tr>
<td>12/4/2015</td>
<td>CBMF, China</td>
<td>CBMI, U.S.</td>
<td>$350,000.00</td>
</tr>
<tr>
<td>1/20/2016</td>
<td>CBMF, China</td>
<td>CBMI, U.S.</td>
<td>$80,000.00</td>
</tr>
<tr>
<td>2/3/2016</td>
<td>CBMF, China</td>
<td>CBMI, U.S.</td>
<td>$70,000.00</td>
</tr>
<tr>
<td>2/5/2016</td>
<td>CBMF, China</td>
<td>CBMI, U.S.</td>
<td>$70,000.00</td>
</tr>
<tr>
<td>3/14/2016</td>
<td>CBMF, China</td>
<td>CBMI, U.S.</td>
<td>$70,000.00</td>
</tr>
<tr>
<td>4/5/2016</td>
<td>CBMF, China</td>
<td>CBMI, U.S.</td>
<td>$20,000.00</td>
</tr>
<tr>
<td>4/11/2016</td>
<td>CBMF, China</td>
<td>CBMI, U.S.</td>
<td>$50,000.00</td>
</tr>
<tr>
<td>5/5/2016</td>
<td>CBMF, China</td>
<td>CBMI, U.S.</td>
<td>$70,000.00</td>
</tr>
<tr>
<td>6/1/2016</td>
<td>CBMF, China</td>
<td>CBMI, U.S.</td>
<td>$70,000.00</td>
</tr>
<tr>
<td>7/1/2016</td>
<td>CBMF, China</td>
<td>CBMI, U.S.</td>
<td>$100,000.00</td>
</tr>
<tr>
<td>8/2/2016</td>
<td>CBMF, China</td>
<td>CBMI, U.S.</td>
<td>$100,000.00</td>
</tr>
<tr>
<td>9/8/2016</td>
<td>CBMF, China</td>
<td>CBMI, U.S.</td>
<td>$70,000.00</td>
</tr>
<tr>
<td>10/14/2016</td>
<td>CBMF, China</td>
<td>CBMI, U.S.</td>
<td>$80,000.00</td>
</tr>
<tr>
<td>11/7/2016</td>
<td>CBMF, China</td>
<td>CBMI, U.S.</td>
<td>$69,985.00</td>
</tr>
<tr>
<td>12/7/2016</td>
<td>CBMF, China</td>
<td>CBMI, U.S.</td>
<td>$100,000.00</td>
</tr>
<tr>
<td>1/9/2017</td>
<td>CBMF, China</td>
<td>CBMI, U.S.</td>
<td>$100,000.00</td>
</tr>
<tr>
<td>2/6/2017</td>
<td>CBMF, China</td>
<td>CBMI, U.S.</td>
<td>$100,000.00</td>
</tr>
<tr>
<td>3/3/2017</td>
<td>CBMF, China</td>
<td>CBMI, U.S.</td>
<td>$100,000.00</td>
</tr>
<tr>
<td>4/7/2017</td>
<td>CBMF, China</td>
<td>CBMI, U.S.</td>
<td>$59,752.67</td>
</tr>
<tr>
<td>4/12/2017</td>
<td>CBMF, China</td>
<td>CBMI, U.S.</td>
<td>$40,000.00</td>
</tr>
<tr>
<td>5/15/2017</td>
<td>CBMF, China</td>
<td>CBMI, U.S.</td>
<td>$70,000.00</td>
</tr>
</tbody>
</table>

Total Transfers $3,109,738.67
indicted, from his personal email account, emailed OGOE at OGOE’s CBMI account the following information: “Sam Please see attach for helpful info.” Attached to the email were seven files. One of the attachments was Trade Secret 1, and one of the tabs included Company A’s logo and name.

C. In or about January 2015, UCHE, from his Company A email account, sent Trade Secret 2 to his personal email account.

D. On or about January 14, 2015, UCHE, from his personal email account, emailed OGOE at OGOE’s CBMI email account Trade Secret 2.

E. In or about January 2015, OGOE removed Company A’s logo and name from Trade Secret 1.

F. On or about January 28, 2015, OGOE sent the revised Trade Secret 1 to SHI.

G. On or about January 30, 2015, UCHE sent an email from his personal email account to OGOE at OGOE’s CBMI email account with the subject “Test procedure.” Attached to the email was Trade Secret 3.

H. On or about March 20, 2015, OGOE emailed SHI, BO, and another CBMI employee, stating the 10mm carbon coated sphere densities for the hydrostatic burst pressure test in China were attached. OGOE also noted the pressure test procedure was attached for their review prior to sending them to China. The email had two attachments, including a Word document titled “Hydrostatic Burst Pressure Test Procedure,” and a spreadsheet titled “Sam-10 mm Carbon Density 3-20-15.” The word document contained a summarized version of the contents of Trade Secret 3.
I. On or about March 21, 2015, BO forwarded OGOE’s March 20, 2015 email, which contained a summarized version of the contents of Trade Secret 3, to HUANG at CBMF in China.

J. On or about March 23, 2015, SHI sent an email titled “Hydrostatic Burst Pressure Test Procedure” to HUANG at CBMF in China and copied BO and U.S. Person 2, an unindicted co-conspirator. The email attached two documents titled “Hydrostatic Burst Pressure Test Procedure 10mm OD” and “Hydrostatic Burst Pressure Test Procedure 4mm OD.” The attachments were substantially similar to the Word document transmitted by OGOE on March 20, 2015, which contained a summarized version of Trade Secret 3.

K. On or about March 26, 2015, HUANG responded to the March 21, 2015 email, which contained the summarized version of Trade Secret 3, by emailing BO and stating, “Attached is the pressure testing report for 10mm carbon coated spheres.”

L. On or about March 26, 2015, BO forwarded HUANG’s March 26, 2015 email, sent in the same email chain containing the summarized version of Trade Secret 3, to OGOE.

M. On or about April 21, 2015, HUANG sent an email to SHI and BO with the results of testing 100 microspheres, stating only 20 of the microspheres passed the test and asked to know the pressure requirements that should be applied in the test.

N. On or about April 10, 2015, SHI, who owned another company, Company B, and who was associated with another company, Company C, sent an email to his
Company B email account. The subject of the email was “Confirm: Interview with Shan SHI at [Company C] 04/09 (Thur) 10:30 am.” The email contained a forward of a message from LIU, who had recently been laid off by Company A, to SHI’s email account at Company C. In the original message, LIU introduced himself and explained a friend referred him to U.S. Company C and SHI. LIU asked to confirm the date/time of his interview at U.S. Company C. The email contained LIU’s resume, which outlined LIU’s employment at Company A.

O. On or about April 12, 2015, SHI, from his Company B email account, emailed LIU to offer a full time job at Company B, in part to mask LIU’s involvement with CBMI from the knowledge of Company A.

P. On or about April 12, 2015, LIU accepted the offer to work at Company B.

Q. On or about April 14, 2015, HUANG tasked SHI and BO via email regarding the manufacture of syntactic foam. The email, in part, stated, “I need information regarding formula, preparation process and performance of the syntactic materials.”

R. On or about April 15, 2015, LIU, from his ODI email account, emailed Trade Secret 4 to SHI at SHI’s CBMI account.

S. On or about April 16, 2015, SHI, in response to LIU’s April 15, 2015 email, emailed LIU at LIU’s Company B email account, asking that LIU “verify the attached material.”

T. On or about April 17, 2015, LIU, from his Company B email account, in response to SHI’s April 16, 2015 email, emailed SHI Trade Secret 5.
U. On or about May 8, 2015, LIU, from his Company B email account, emailed SHI, BO, and HUANG Trade Secret 6.

V. On or about June 4, 2015, LIU emailed HUANG Trade Secret 7, stating, “The attachment provides technical data of the raw materials and prices of part of the raw material received by [Company A] for your reference.”

W. On or about June 20, 2016, U.S. Person 2, an unindicted co-conspirator, emailed CBMI’s accountant and instructed the accountant to “stop Gang LIU’s [Company B] payroll from June 1 [2016]” because LIU was transferred to CBMI’s system.

**Marketing and Developing Military and PRC Uses of CBMF Products**

X. On or about May 19, 2016, LIU emailed SHI and BO a PowerPoint presentation, which outlined the military and civilian applications of buoyancy material and asked for their edits.

Y. On or about May 24, 2016, SHI emailed HUANG and U.S. Person 2, an unindicted co-conspirator, a Word document which outlined CBMF’s “Outlook on Composite Buoyancy Material Product in Military Application.”

Z. On June 6, 2016, HUANG emailed LIU a CBMF PowerPoint presentation stating that CBMF provided light composite materials usable for, among other items, armor, and that CBMF products were suitable for naval vessels core materials and island reef building, as well as for armored vehicles.

AA. On or about July 5, 2015, U.S. Person 2, an unindicted co-conspirator, sent an email to SHI and copied HUANG and LIU. The email was titled “Re: Deep
water drilling riser buoyancy module product research and development program.” The email attached a document laying out CBMF’s strategy regarding DRBM R&D and noted CBMF’s goal to support the development of marine equipment for the PRC’s next “Five-Year Plan.” The document announced in part that CBMF has planned to design a set of a large deepwater hydrostatic pressure test systems that matched the international advanced technology level within one year.

Use of Patents

BB. On or about August 21, 2015, HUANG emailed SHI and U.S. Person 2, an unindicted co-conspirator, questions regarding a sphere patent application. HUANG suggested three options regarding the inventor. HUANG stated that although the technical portion of the sphere originated from LIU, the patent office thought LIU was not an appropriate choice because he was still within the period of his non-compete clause period with Company A; therefore, it was against the law. HUANG stated someone needed to explain this to LIU. The second choice would be SHI or U.S. Person 2, and since they had no official contract with Company A, the risk was manageable. The third choice would be HUANG as a representative of Chinese staff.

CC. On or about September 22, 2015, CBMF, with named inventors HUANG and U.S. Person 2, an unindicted co-conspirator, applied for a patent with the State Intellectual Property Office of the PRC.

Development of CBMF’s Factory

DD. On or about September 16, 2015, OGOE traveled to China.
EE. On or about October 1, 2015, OGOE sent an email to BO titled “Greetings from [CBMF] Factory.” OGOE asked how his colleagues in the United States were doing and stated, “We are at the factory gladly working to get the task accomplished.”

FF. On or about October 17, 2016, SHI called U.S. Person 3 about CBMF. SHI explained he had a factory in China that produces buoyancy material. SHI stated the business was doing very well, and the competitors had died off. SHI stated they were becoming a bigger company and said, “We standout and everybody come to see us now to try to get cheap product.” SHI also stated he hired a whole bunch of people in the United States that “really know how [to develop buoyancy material].”

**Relationship with Company A**

GG. In or about the Fall of 2015, SHI sought to sell macrospheres to Company A and entered into negotiations with employees of Company A.

HH. In or about the Fall of 2015, SHI touted CBMF to Company A as a high profile collaboration with the PRC Government.

II. In or about the Fall of 2015, SHI also touted CBMF to Company A as connected to HEU.

JJ. In December of 2015, when Company A employees visited the CBMF facility to further investigate whether to purchase macrospheres from CBMF, SHI stated that CBMF was a high profile project for the PRC Government, that the PRC Government had invested a lot in CBMF, and that China would not allow CBMF to fail.
On or about October 24, 2016, PRC-Person 1, an unindicted co-conspirator, emailed SHI asking him to strengthen ties with Company A. PRC-Person 1 told SHI to find out whether CBMF could sell the Company A foam balls and the microspheres, and they need to know Company A’s moves in order to adjust CBMF’s business strategy.

Rig Contract

In or about September or October of 2016, SHI traveled to China to present CBMF’s technical capabilities to a CNOOC subsidiary, in response to a request for proposal for repair of drill riser buoyancy modules on an oil rig (“Rig Contract”).

On or about December 29, 2016, HUANG forwarded an email to SHI to LIU, which was an email from the CNOOC subsidiary with technical blueprints for the request for proposal, which included information that some of the foam needed to be functional at depths of more than 1,000 meters with a density lighter than 561 kg/m3,

On or about January 18, 2017, after agents from the Department of Commerce notified SHI about export law rules pertaining to syntactic foam, SHI confirmed with BO that if the formula was outside of a certain range, they had to apply for a permit to export the formula to the PRC.

On or about January 19, 2017, SHI informed the Department of Commerce that he would study the email with BO, and would advise if there were any questions, referencing an email SHI received from the Department of Commerce providing attached export control information and stating that technology related
to the development, production, or use of syntactic foam at specified levels would require a license for export,

PP. On or about between January 2017 and February 15, 2017, CBMF, CBMI, SHI, LIU, and other members of the conspiracy, both known and unknown to the grand jury, continued to work on the Rig Contract.

**CBMI Bid**

QQ. On or about May 15, 2017, LIU provided to BO a list of projects that CBMI had previously completed, including Autonomous Underwater Vehicle (“AUV”) research for HEU, and other syntactic foam projects for CSIC and CNOOC. Line 1 of the list of projects was “AUV Research” for HEU.

RR. On or about May 15, 2017, BO, SHI, and LIU submitted a CBMI bid on a contract for the next generation of commercial Remote Operated Vehicles (“ROV”) for U.S. Company D, a corporation. CBMI’s bid included the previously referenced list of projects that CBMF had completed. The contract required that the ROVs had to attain depths of 4,000-6,000 meters and that the foam had to have a density less than 550 kg/m3.

SS. On or about May 22, 2017, Shi sent an email to HUANG, stating that CBMI would be meeting to bid for the Company D project, and that CBMI had been asked to provide testimonials or references from previous syntactic foam customers referred to in the May 15, 2017 list of projects.

TT. On or about May 23, 2017, SHI, LIU, and U.S. Person 4 traveled to Washington, D.C. in order to present CBMI’s bid.
UU. On or about May 23, 2017, in the District of Columbia, SHI, LIU and U.S. Person 4 provided a briefing of CBMF and CBMI’s capabilities to U.S. Company E, an entity purporting to represent U.S. Company D, as part of CBMF and CBMI’s bid for the U.S. Company D project.

VV. On or about May 23, 2017, in the District of Columbia, during the briefing, LIU and SHI discussed CBMF and CBMI’s previous projects. LIU stated the project closest to the specifications requested by Company D was a deepwater project for CNOOC that involved providing syntactic foam.

WW. On or about May 23, 2017, in the District of Columbia, during the powerpoint presentation of previous projects, LIU noted a photo of steel buoys containing syntactic foam produced by CBMF. LIU stated “I don’t know if we can put it there [in the powerpoint], it’s military use.” When asked to clarify if LIU meant the Chinese military, LIU laughed and said “skip it.” SHI stated “We try not to work for the military.”

XX. On or about May 23, 2017, HUANG sent to SHI photographs of the AUV built for HEU and listed in line 1 of the list of projects, which appear to be related to the project described in paragraph 38 QQ. A logo on the AUV is for KLSTND, which is further described in paragraph 2.

*(Conspiracy to Commit Theft of Trade Secrets, pursuant to Title 18, United States Code, Section 1832(a)(5))*
COUNT TWO

(Conspiracy to Commit Economic Espionage)

39. The allegations in Paragraphs 1 through 33, and 36 through 38 (including the Overt Acts, and the Ways, Manners and Means) of this Indictment are incorporated and re-alleged by reference herein.

40. Beginning on a date unknown to the Grand Jury but at least by, in or about March 2012, and continuing until on or about May 23, 2017, in the District of Columbia, and elsewhere, the defendants, SHI, LIU, CBMF, CBMI, and others both known and unknown to the grand jury did knowingly and willfully combine, conspire, confederate, and agree with each other, and others known and unknown to the Grand Jury, to commit the following offenses:

A. Intending and knowing that the offense will benefit any foreign government, foreign instrumentality, and foreign agent, knowingly steal, and without authorization appropriate, take, carry away, and conceal, and by fraud, artifice, and deception obtain a trade secret, in violation of Title 18, United States Code, Section 1831(a)(1);

B. Intending and knowing that the offense will benefit any foreign government, foreign instrumentality, and foreign agent, knowingly, and without authorization copy, duplicate, sketch, draw, photograph, download, upload, alter, destroy, photocopy, replicate, transmit, deliver, send, mail, communicate, or convey a trade secret in violation of Title 18, United States Code, Section 1831(a)(2); and

C. Intending and knowing that the offense will benefit any foreign
government, foreign instrumentality, and foreign agent, knowingly receive, buy, or possess a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization, in violation of Title 18, United States Code, Section 1831(a)(3).

(Conspiracy to Commit Economic Espionage, pursuant to Title 18, United States Code, Section 1831(a)(5))

OBJECTS OF THE CONSPIRACY

41. The objects of the conspiracy were:
   A. To appropriate trade secrets belonging to Company A for the benefit of the PRC;
   B. To replicate trade secrets belonging to Company A for the benefit of the PRC; and
   C. To receive and possess trade secrets belonging to Company A for the benefit of the PRC.

COUNT THREE

(Conspiracy to Launder Monetary Instruments)

THE CONSPIRACY

42. The allegations in Paragraphs 1 through 33, and 36 through 38 of Count One of this Indictment, including the Overt Acts, and the Ways, Manner and Means, are incorporated and re-alleged by reference herein.

43. Beginning as early as in or around 2014, the exact date being unknown to the Grand Jury, and continuing through in or around May 2017, within the extraterritorial jurisdiction of the
United States, the District of Columbia, and elsewhere, defendants SHAN SHI, CBMF, CBMI, and others known to the grand jury did knowingly, combine, conspire, confederate and agree with others, known and unknown to the Grand Jury, to violate Title 18, United States Code, Section 1956(a)(2)(A), that is, to transport, transmit, and attempt to transport, transmit, and transfer, monetary instruments and funds to or through a place in the United States from or through a place outside the United States, that is, China, with the intent to promote the carrying on of specified unlawful activities, that is, violations of 18 U.S.C. §§ 1831-1832 (relating to economic espionage and theft of trade secrets).

THE OBJECTS OF THE CONSPIRACY

44. The objects of the conspiracy were:
   A. to promote the co-conspirators’ illegal scheme; and
   B. to illegally enrich the co-conspirators.

MANNER AND MEANS OF THE CONSPIRACY

45. The manner and means by which SHI, CBMF, CBMI, and other co-conspirators sought to accomplish the objects of the conspiracy included, among others, the following:
   A. SHI, CBMF, CBMI, and others known and unknown to the grand jury planned and acted outside of the United States to acquire U.S.-origin technology from U.S. companies.
   B. SHI, CBMF, CBMI, and others known and unknown to the grand jury did this by stealing trade secrets. Such technology was ultimately destined to the PRC.
   C. CBMF wired money from accounts outside the United States to accounts of CBMI inside the United States, to promote this scheme.
46. It was part of the conspiracy that SHI, CBMF, CBMI, and other co-conspirators known and known to the grand jury engaged in illegal financial transactions totaling at least $3,109,738.67 involving the above-identified criminally-derived property, by wiring funds into the United States to promote the theft of trade secrets. The list of transactions at paragraph 38 a) are incorporated herein.

(Conspiracy to Launder Monetary Instruments, in violation of Title 18, United States Code, Section 1956(h).)

FORFEITURE ALLEGATION

1. Upon conviction of either offense alleged in Count One or Count Two, the defendants shall forfeit to the United States: (a) any article, the making or trafficking of which is prohibited by 18 U.S.C. §§ 1831, 1832, (b) any property used, or intended to be used, in any manner or part to commit or facilitate the commission of the offense alleged in Count One or Count Two; and (c) any property constituting or derived from any proceeds obtained directly or indirectly as a result of the commission of the offense alleged in Count One or Count Two, pursuant to 18 U.S.C. § 2323; and (d) any property, real or personal, which constitutes or is derived from proceeds traceable to these offenses, pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c). The United States will also seek a forfeiture money judgment against the defendants of at least $3,109,738.67.

2. Upon conviction of the offense alleged in Count Three, the defendants shall forfeit to the United States any property, real or personal, involved in such offense, or any property traceable to such property, pursuant to 18 U.S.C. § 982(a)(1). The United States will also seek a forfeiture money judgment against the defendant of at least $3,109,738.67.4. The Grand Jury finds
by probable cause that the following specific properties are subject to forfeiture upon conviction of the offense alleged in Counts One through Three:

A. real property located at 7 Buckingham Court, Houston, Texas, with all appurtenances, improvements, and attachments thereon, and is more fully described as: Lot 7, of Buckingham Court, a subdivision in Harris County, Texas, according to the map and plat thereof, recorded in Film Code No. 347064 of the map records of Harris County, Texas;

B. real property located at 13601 Farm To Market 529, Houston, Texas, with all appurtenances, improvements, and attachments thereon, and is more fully described as – a tract of land containing 2.5727 acres of land (112,067 sq.ft.) out of the Charles Scarbrough survey, Abstract No. 718, being a portion of a 4.000 acre tract of land as recorded under Harris County Clerk’s file No. (CCFN) 20100135228 of the official public records of Harris County, Texas;

C. any and all funds in Bank of America account 586035464818;

D. any and all funds in Bank of America account 586033253050; and

E. any and all funds in Bank of America account 586033316528.

3. If any of the property described above as being subject to forfeiture, as a result of any act or omission of the defendant:

A. cannot be located upon the exercise of due diligence;

B. has been transferred or sold to, or deposited with, a third party;

C. has been placed beyond the jurisdiction of the Court;

D. has been substantially diminished in value; or
E. has been commingled with other property that cannot be divided without difficulty;

the defendant shall forfeit to the United States any other property of the defendant, up to the value of the property described above, pursuant to 21 U.S.C. § 853(p).

(Criminal Forfeiture, pursuant to Title 18, United States Code, Sections 981(a)(1)(C), 982, and 2323; Title 21, United States Code, Section 853(p); and Title 28, United States Code, Section 2461(c).)

A TRUE BILL

FOREPERSON

[Signature]
Attorney of the United States in
and for the District of Columbia