

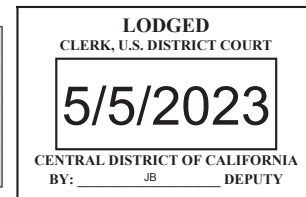
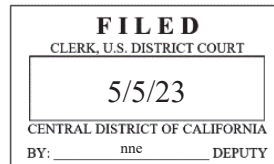
AO 91 (Rev. 11/11) Criminal Complaint (Rev. by USAO on 3/12/20)

Original Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California



United States of America

v.

LIMING LI,

Defendant.

Case No. 5:23-mj-00223 -DUTY

CRIMINAL COMPLAINT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

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 September 9, 2020, in the county of San Bernardino in the Central District of California, the defendant violated:

Code Section

18 U.S.C. § 1832

Offense Description

Theft of Trade Secrets

This criminal complaint is based on these facts:

Please see attached affidavit.

Continued on the attached sheet.

/s/ Katherine Miller

Complainant's signature

Katherine Miller, FBI Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date:

May 5, 2023

Judge's signature

City and state: Los Angeles, California

Hon. Maria A. Audero, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT

I, KATHERINE MILLER, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and has been so employed since 2021. I am currently assigned to the Los Angeles Field Office, West Covina Resident Agency. Prior to joining the FBI, I was employed for four years as a sworn member of the D.C. Metropolitan Police Department. I am currently assigned to a squad tasked with investigating counterintelligence threats relating to the People's Republic of China ("PRC"). In this role, I have been involved in investigating, among other violations, the theft of trade secrets, malign foreign influence operations, and the illegal export of key technologies from the United States. Based on my experience and training, I am familiar with efforts and techniques used to unlawfully collect trade secret information.

II. PURPOSE OF AFFIDAVIT

2. I make this affidavit in support of a criminal complaint and arrest warrant against Liming Li ("LI") for a violation of 18 U.S.C. § 1832: Theft of Trade Secrets.

3. This affidavit is also made in support of an application for a warrant to search the person of LI, as described more fully in Attachment A, for evidence, fruits and instrumentalities of violations of the following statutes, as described more fully in Attachment B, which is also incorporated herein by reference: 50 U.S.C. § 1705 (International Emergency

Economic Powers Act); 15 C.F.R. §§ 730-774 (the Export Administration Regulations); 50 U.S.C. §§ 4801-4852 (Export Control Reform Act); 18 U.S.C. § 1831 (Economic Espionage); and 18 U.S.C. § 1832 (Theft of Trade Secrets) (collectively, the "SUBJECT OFFENSES").

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only and all dates and times are approximate.

III. SUMMARY OF PROBABLE CAUSE

5. Between 1996 and November 2019, Liming Li ("LI") worked in various engineering, management, and software development roles for two companies in southern California that develop and sell Computer Aided Design ("CAD") software programs related to High Precision Metrology Interpretation and Point Cloud Technology. These technologies can be used in various sensitive manufacturing contexts, including manufacturing parts for nuclear submarines and military aircraft, and are subject to United States export controls for national security, nuclear nonproliferation, and anti-terrorism reasons.

6. LI worked for the first company ("COMPANY #1") from 1996 to 2018 and for the second company ("COMPANY #2") from 2018 to November 2019. Shortly before beginning his employment with COMPANY #2, LI and his wife established their own smart manufacturing company, JSL INNOVATIONS.

7. After LI was terminated by COMPANY #2, company security found that LI was using his company-issued laptop to attempt to download files from COMPANY #2's root directory onto his personal external hard drive. After company security had LI removed from the premises, they searched his company-issued laptop and found a folder labeled "ChinaGovernment." That folder contained numerous documents showing LI's efforts to participate in the PRC's Thousand Talents Program and to use his own company, JSL INNOVATIONS, to provide to PRC business and government entities export-controlled and trade secret technology related to the work of COMPANY #1 and COMPANY #2.

8. In March 2020, LI entered an agreement with a manufacturing company based in Suzhou, Jiangsu Province, in China ("PRC EMPLOYER-1") to serve as Chief Technical Officer to help the company develop software for smart manufacturing.

9. In September 2020, FBI agents executed a search warrant at LI's home and found numerous digital devices containing millions of files belonging to COMPANY #1 and COMPANY #2 and containing the source code for those companies' proprietary software. Although the source code files had been developed by and belonged to COMPANY #1 and COMPANY #2, certain of the files had been moved into folders labeled JSL or JSL

Projects, among other things. In an interview with FBI agents, LI initially denied possessing any source code belonging to COMPANY #1 or COMPANY #2, but later admitted that he did possess such source code and had referenced it to build his own software source code for JSL INNOVATIONS. As detailed below, both COMPANY #1 and COMPANY #2 derive significant value from the secrecy of their proprietary software source code, and take extensive steps to protect the source code from discovery by competitors.

10. LI's agreement with PRC EMPLOYER-1 required that he spend at least six months per year in the PRC to support the joint project. In 2020, LI attempted to fly to the PRC on a flight arranged by PRC EMPLOYER-1 but was unable to do so due to the COVID-19 pandemic. In February 2023, LI flew to Taiwan on the same itinerary that PRC EMPLOYER-1 had previously provided him. He is scheduled to return to the United States on May 6, 2023. During his travel, LI has had several email communications with a representative of PRC EMPLOYER-1. For these reasons, as detailed further below, I believe that the purpose of the LI's trip was to meet with PRC EMPLOYER-1 in furtherance of their agreement to develop smart manufacturing software, including through LI's use of the trade secrets LI stole from COMPANY #1 and COMPANY #2, and that evidence related to that illegal activity is likely to be contained on LI's person, including his digital devices.

IV. LEGAL BACKGROUND ON EXPORT AND TRADE SECRET OFFENSES

A. IEEPA

11. The International Emergency Economic Powers Act ("IEEPA"), 50 U.S.C. §§ 1701-1707, grants the President of the United States ("the President") the authority to regulate exports and other international transactions in times of national emergency. IEEPA controls are triggered by an Executive Order declaring a national emergency based on an "unusual and extraordinary threat, which has its source in whole or substantial part outside the United States, to the national security, foreign policy, or economy of the United States." Pursuant to the authority under IEEPA, the President and the executive branch have issued orders and regulations governing and prohibiting certain practices and transactions with respect to various sanctioned nations by U.S. persons or involving U.S.-origin goods.

12. Pursuant to IEEPA, 50 U.S.C. § 1705(a), (c), it is a crime for a person to willfully commit, willfully attempt to commit, willfully conspire to commit, or willfully cause a violation of any license, order, regulation, or prohibition issued under IEEPA.

B. The Export Administration Regulations

13. On August 17, 2001, under the authority of IEEPA, the President issued Executive Order 13222, which declared a national emergency with respect to the unrestricted access of foreign parties to U.S. goods and technologies, and continued in effect the EAR, 15 C.F.R. §§ 730-774. The President has issued

annual Executive Notices extending the national emergency declared in Executive Order 13222 from the time period covered by the Executive Order through the present. See, e.g., 84 Fed. Reg. 41881 (Aug. 15, 2019).

14. Among other things, the EAR controls the export and re-export to foreign countries of commercial items that also have a military application. The EAR places limitations on the export of those goods and technology that the Secretary of Commerce deems could make a significant contribution to the military potential of other countries, could prove detrimental to the national security of the United States, or contrary to the foreign policy of the United States. The Department of Commerce maintains the Commerce Control List ("CCL"), which specifies the most sensitive goods and technologies subject to the EAR. Items on the CCL are identified by an Export Control Classification Number ("ECCN") that sets forth a description of the controlled commodity or technology, its licensing requirements, any potential license exceptions, and the reasons for its export control. Depending on the nature of the item, the destination country, the end-use, and the end-user of the item, a validated license from the Department of Commerce's Bureau of Industry and Security (or "BIS," as noted above) may be required for export.

15. As noted above, each ECCN specifies the applicable reasons for control (such as national security, short supply, anti-terrorism, etc.). By referencing the reasons for control set forth in the applicable ECCN, the Commerce Country Chart

specifies for which countries a license is required before a commodity may be exported there. See 15 C.F.R. § 738, Supp. No. 1.

16. Under the EAR, "technology" may be in any tangible or intangible form, such as written or oral communications, blueprints, drawings, photographs, plans, diagrams, models, formulae, tables, engineering designs and specifications, computer-aided design files, manuals or documentation, electronic media or information revealed through visual inspection.

17. Part 742 of the EAR describes CCL-based controls according to the reasons for control reflected in the headings on the Commerce Country Chart. This chart lists every country with a cross-reference for each control. These controls generally described when a license is required for shipment to a certain country based on a certain control. It also describes more specific licensing policies for certain controls. Under the heading for National Security, there are licensing requirements and policies with respect to particular ECCNs.

18. Finally, the Violations section of the EAR specifically describes under the misrepresentation and concealment of facts heading that:

No person may make any false or misleading representation, statement, or certification, or falsify or conceal any material fact, either directly to BIS, the United States Customs Service, or an official of any other United States agency, or indirectly through any other person...For the purpose of or in connection with effecting an export, reexport or other activity subject to the EAR.

And:

All representations, statements, and certifications made by any person are deemed to be continuing in effect. Every person who has made any representation, statement, or certification must notify BIS and any other relevant agency, in writing, of any change of any material fact or intention from that previously represented, stated, or certified, immediately upon receipt of any information that would lead a reasonably prudent person to know that a change of material fact or intention has occurred or may occur in the future.

15 C.F.R. § 764.2.

C. The Export Control Reform Act

19. On August 13, 2018, the President signed into law the National Defense Authorization Act of 2019, which includes provisions on export controls, entitled the Export Control Reform Act of 2018 ("ECRA"), Pub. L. No. 115-232, tit. 17, subtitle B, 132 Stat. 2208 (2018). This has since been codified at 50 U.S.C. §§ 4801-4852. In part, ECRA provides permanent statutory authority for the EAR and eliminates the need for the President to declare annually national emergencies pursuant to IEEPA and Executive Order 13222. For conduct that predates August 13, 2018, IEEPA is the controlling statute. For conduct occurring after August 13, 2018, ECRA is the controlling statute.

D. Economic Espionage

20. Based on my training and experience, I know the following. Title 18, United States Code, Section 1831 (Economic Espionage) provides in relevant part:

(a) In General—Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly—

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;

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

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

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

(5) conspires with one or more other persons to commit any offense described in any of 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 not more than \$5,000,000 or imprisoned not more than 15 years, or both.

21. I am further advised that the term "foreign government" as used in 18 U.S.C. § 1831 is defined by 18 U.S.C. § 11 as "any government, faction, or body of insurgents within a country with which the United States is at peace, irrespective of recognition by the United States."

22. I am further advised that the term "foreign instrumentality" as used in 18 U.S.C. § 1831 is defined by 18 U.S.C. § 1839(1) as "any agency, bureau, ministry, component, institution, association, or any legal, commercial, or business organization, corporation, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government."

E. Theft of Trade Secrets

23. Based on my training and experience, I know the following. Title 18, United States Code, Section 1832 (Theft of Trade Secrets) provides:

(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.

24. Title 18, United States Code, Section 1839(3) and (4) defines the term "trade secret" as:

(3) [T]he term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether

tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if-

(A) the owner thereof has taken reasonable measures to keep such information secret; and

(B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public[.]

(4) [T]he term "owner", with respect to a trade secret, means the person or entity in whom or in which rightful legal or equitable title to, or license in, the trade secret is reposed.

V. STATEMENT OF PROBABLE CAUSE

A. Background on the Thousand Talents Plan

25. From my training and experience, and based on my review of reports, I understand that the PRC government has established so-called "Talent Programs" through which it identifies individuals located outside the PRC who have expert skills, abilities, and knowledge that would aid in transforming the PRC's economy. These programs, which have existed since the early 1990s, recruit such individuals to work on behalf of the PRC. The Talent Programs were reemphasized as a national strategy for Chinese economic development in 2007 when "talent development" was added to the Constitution of the Communist Party of China ("CPC").

26. In 2008, the PRC Government published "Advice for Implementing the Recruitment Program of Global Experts," and, in 2009, published official guidance on the Talent Program application process, identifying multiple levels of governmental review for all applicants. The CPC Organization Department conducts the final review of all Talent Program applicants. In

addition, the Chinese government directly administers and funds the Talent Programs, using other agencies within the government to ensure implementation of strategic national objectives.

27. Currently, there are believed to be over two hundred Chinese Talent Programs, including plans tailored for ethnic Chinese, non-ethnic Chinese, established scientists, young scientists, and entrepreneurs, among others. Each Talent Program includes the same basic requirements: the applicant should have experience in cutting-edge foreign science or engineering research; possess a degree from a prestigious university; and have several years of overseas work or research experience at prestigious universities, research institutes, corporations, or well-known enterprises.

28. In 2016, the PRC press reported more than 56,000 total Talent Program recruits ("Talent Recruits") in numerous programs, many of which are specific to particular regions or cities of the PRC. The seminal, national-level Talent Program was initiated in 2009. It is officially known as the Recruitment Program of Global Experts, and it is commonly referred to as the Thousand Talents Program. Through the Thousand Talents Program, the PRC government recruits Western-educated individuals to work and conduct technical and scientific research on behalf of PRC and in furtherance of the PRC's strategic national development goals.

29. The Chinese Talent Program application process is conducted almost exclusively via digital communications, and primarily occurs through email. Various websites provide the

necessary information to apply, including digital application forms. Talent Program applicants complete applications and send them electronically to individuals identified by the PRC government as so-called Talent Recruiters in the United States and China. Talent Recruits and Talent Recruiters then refine Talent Program draft applications using various forms of digital communication. In some cases, a Talent Recruiter asks an applicant for information about the work the applicant performs or has performed, including materials the Talent Recruiter knows to be sensitive, the proprietary intellectual property of a company, or requiring a license for export from the United States to the PRC. PRC government guidance on Talent Program applications provides that Talent Recruits must provide evidence of the work they performed on projects they list on their applications, such as research results or innovative achievements.

30. To entice high-caliber applicants—particularly applicants willing to relocate to the PRC, the PRC government rewards Talent Recruits with significant financial and social incentives. Each Talent Recruit draws a salary from a PRC-based employing unit, such as a laboratory or research organization, which sponsors or facilitates applications. These salaries often meet or exceed salaries the Talent Recruits draw through their non-PRC employment. For Thousand Talent Program Recruits, the PRC government has been known to provide as much as \$150,000 as a signing bonus, and an additional \$450,000–\$750,000 over time to support research. Additional funding is available,

depending on the Talent Recruit's level of expertise and quality of performance in meeting Talent Program goals. The PRC government may also supply free housing or a generous housing allowance, high-quality schooling for children, jobs for spouses, healthcare, and significant tax breaks.

31. Talent Recruits sign contracts covering their participation in Talent Programs. These contracts obligate the Recruits to work for a specified period in the PRC, and often detail the specific research the Talent Recruit will perform or specify the business that is to be developed by the proposed new company. This contractual obligation closely resembles or even replicates the work the Talent Recruit performs or performed for his or her U.S. employer, thus demonstrating the Talent Recruit's willingness to leverage knowledge and intellectual property obtained from U.S. businesses, corporations, and even U.S. government laboratories. In many cases, Talent Program contracts also require Talent Recruits to identify additional overseas talent to join his or her Talent Program research team in the PRC, resulting in a cell-based recruitment model in which Talent Recruits also become de facto Chinese Talent Program recruiters. This contractual relationship differentiates Talent Programs from standard scientific research grants or conventional international collaboration.

32. Based on my review of reports, as discussed below, in February 2018, LI documented his planned participation in the Thousand Talent Program through a saved, signed, and completed application found on his COMPANY #2-issued laptop for "Overseas

High-level Talents" ("Overseas Talents"). In October 2018, the "Beijing Overseas Talents Center" held a tour for Overseas Talents for four days, which LI attended. The Beijing tour aimed to attract high-level talent and offer high-quality services in the fields of hospitals, colleges, universities, enterprises, R&D projects, and commercialization. In his application to participate in that tour, LI listed his employer as JSL INNOVATIONS and described his background in CAD, measuring/survey software, COMPANY #1 model-based metrology software, Point Cloud Analysis modules, and experience in Model-Based Design Metrology software systems. LI provided a short paragraph on the application document which described his goals and objectives for the Talent Program: "promote smart manufacturing implementation for Chinese Enterprise."

B. 1996-2019: LI Works for U.S. Companies Developing Software for Smart Manufacturing and Develops His Own Company, JSL INNOVATIONS

33. According to COMPANY #1 records, from 1996 to 2018, LI worked in various engineering and management roles for companies under the umbrella of COMPANY #1, an international firm with offices throughout the United States. According to COMPANY #2 records, from in or about 2018 until November 2019, LI worked as Software Development Director for COMPANY #2. According to company employees, COMPANY #1 and COMPANY #2 develop and sell EAR-controlled CAD software programs related to High Precision Metrology Interpretation and Point Cloud Technology. The technology is used for various manufacturing purposes, including in sensitive contexts such as parts for nuclear submarines and

military aircraft, and it is colloquially referred to as a component of advanced or "smart" manufacturing. According to COMPANY #1 and COMPANY #2, the source code for their proprietary software programs constitutes valuable trade secrets, and they take extensive steps to protect the secrecy of the source code, as detailed further below.

34. In or about around January 2018, LI was terminated from his position as Chief Technologist for a subsidiary of COMPANY #1.

35. According to California Secretary of State business records, in February 2018 LI's wife J.J. incorporated JSL INNOVATIONS, using her and LI's shared residence as the place of business. The incorporation documents state that JSL INNOVATIONS performs technology consulting, and list J.J. as the incorporator, owner, CFO, Secretary, and CEO. Based on FBI review of emails between LI, J.J., and others, LI and J.J. marketed JSL INNOVATIONS as a technology consulting firm centered on LI's knowledge and experience as a software developer, and described LI as the firm's Chief Technologist.

36. In or about May 2019, LI was hired as a Software Development Director for COMPANY #2. COMPANY #2 specializes in industrial metrology equipment and technology, with particular emphasis on the automotive and aircraft industries. LI was based in the company office in Ontario, California, and was responsible for assembling and managing a team of software engineers working on a computer-aided design program ("D.C.") used to operate COMPANY #2 equipment and instruments, including

coordinate-measuring machines. According to COMPANY #2 representatives, both the software and the equipment were developed and sold by COMPANY #2.

37. In November 2020, BIS evaluated source code files related to propriety COMPANY #2 D.C. software. According to BIS's written response, BIS determined the commodity was subject to EAR controls (15 C.F.R. Part 730 et seq) and classified under ECCN 2E001/2E002, controlled for national security (NS1), nuclear nonproliferation (NP1), and anti-terrorism (AT1) reasons. During the specified timeframe (November 2015 to November 2020), a BIS license was required under the EAR for the export to China of items classified under 2E001/2E002.

C. November 2019: LI is Terminated and Attempts to Download Data from his Work Computer

38. In or about November 2019, a COMPANY #2 principal ("T.S.") terminated LI. In sum and substance, T.S. informed the FBI of the following:

a. In November 2019, T.S. traveled to the COMPANY #2 office in Ontario, California to terminate LI's employment, due to conflicts between LI and the other software engineers. When T.S. informed LI of his termination, LI requested access to his work laptop computer—which was the property of and issued by COMPANY #2—to remove personal photographs and other files unrelated to his work at COMPANY #2 from the device. T.S. permitted LI to remove his personal files from his work computer in the presence of T.S. and another employee, D.M.

b. LI connected a personal external hard drive to the laptop and began to select items to download. At one point, T.S. noticed LI had stopped downloading photographs and started downloading other unknown files from COMPANY #2's root directory. T.S. directed LI to stop downloading materials and had LI removed from the premises. T.S. inspected the root directory on the COMPANY #2 laptop, from which LI had been attempting to remove files, and discovered a folder named "ChinaGovernment." The folder contained multiple applications to Chinese businesses and entities in which it appeared LI was offering to provide COMPANY #2 software. On the device, T.S. also observed what appeared to be proprietary information from LI's previous employer, COMPANY #1.

c. T.S. was concerned LI had misappropriated proprietary information from COMPANY #2 and COMPANY #1, which could be used to the detriment of both companies. T.S. was further concerned because T.S. believed the COMPANY #2 software to be EAR-controlled.

39. In November 2020, BIS also evaluated approximately four slideshow presentations located on LI's digital devices, in which LI appeared to market the products and services of JSL INNOVATIONS to various PRC entities. BIS determined the four presentations contained materials subject to the EAR, including EAR99, due to a presumption of denial.

D. 2016-2018: LI Attempts to Join the Thousand Talents Program

40. Based on my investigation and my review of reports, I am aware of the following. In February 2020, after LI was terminated by COMPANY #2, FBI reviewed a copy of the contents of LI's COMPANY #2-issued laptop. The hard drive contained a sub-folder labeled "ChinaGovernment," within a folder labeled "JSL Projects." Within that folder, FBI agents found several documents related to LI's attempts to join the Thousand Talents Program, including the following:

a. A document dated May 2016, titled "Instruction for the Brief Information of Overseas High-level Talents," providing instructions on how to fill out an application for the PRC Government's Thousand Talents Program;

b. A document dated May 2018, titled "Recruitment Program of Global Experts," which also contained detailed instructions regarding how to apply to the Thousand Talents Program;

c. A document dated June 2018, titled "Brief Information of Overseas High-level Talent," containing LI's picture attached to the front, as well as LI's full name and date of birth;

d. A document dated July 2018, titled "1000 Talent Plan Application (Long Term Program)," containing embedded comments from an unknown administrator requesting clarification of information provided on the application. Based on a preliminary translation, the application was for the 1000 Talents Plan at Hebei Academy of Sciences for industrial software

development in the field of smart manufacturing. The document provided LI's work history, including his tenure at COMPANY #1 and JSL INNOVATIONS. The document listed three patents for which LI identified himself as the owner. Notably, records maintained by the United States Patent Office reveal that LI was listed as the inventor on the three patents, but COMPANY #1 was listed as the assignee. LI stated in the application he had 20 years of experience at COMPANY #1 and wanted to "promote smart manufacturing implementation for Chinese Enterprise." .

e. A draft letter dated June 2018 that appears to be by an official in the Hebei Provincial Government. Based on my training and experience, as well as basic Internet searches, I know the Hebei Provincial Government is directly overseen by the PRC State Council, which is controlled by the CPC. The letter discussed the PRC's urgent need for smart manufacturing software, LI's expertise in the field, and LI's experience as lead software developer for COMPANY #1. The letter stated that the Hebei Province had initiated several Talent Programs and secured funding to establish a Hebei Research Institute of Smart Manufacturing with the goal of rolling out several software products by the end of 2019. The letter listed several specific products, including the GD&T Calculation Model, Point Cloud Analysis module, and MBD Metrology Software. The letter asked the PRC Government to accept LI into the Thousand Talents Program notwithstanding that his age past the standard age limit for applicants.

41. According to information provided by COMPANY #1 and COMPANY #2, the specific products listed in the June 2018 letter appear to be the same as products offered by COMPANY #1 and COMPANY #2.

E. 2018: LI Markets Smart Manufacturing Technology to PRC Entities through JSL INNOVATIONS

42. Based on my investigation and my review of reports, I am aware of the following. Also within the "ChinaGovernment" folder and other folders, FBI agents observed numerous documents showing LI's efforts to provide what appeared to be EAR-controlled and trade-secret technology related to the work of COMPANY #1 and COMPANY #2 to PRC business entities and government entities through JSL INNOVATIONS. For example, agents observed the following:

a. A March 2018 JSL Innovations PowerPoint, written in Mandarin, titled "Marketing Analysis for Potential Projects," which outlined JSL INNOVATIONS' plan in the PRC relevant to "Made in China 2025."¹ The PowerPoint addressed specific smart manufacturing technologies and explained that JSL INNOVATIONS

¹ Based on my training and experience and review of news reports, I know that in 2015, the PRC's State Council issued the Made In China 2025 Notice, a ten-year plan to comprehensively upgrade the Chinese economy through the promotion and development of ten advanced technology industries. The ten advanced technology industries are: (1) Next Generation Information Technology (e.g. Artificial Intelligence, IoT); (2) Robotics and Automated Machine Tools; (3) Aerospace; (4) Maritime Vessel and Maritime Engineering Equipment; (5) Advanced Rail Equipment; (6) Clean Energy Vehicles; (7) Electrical Generation and Transmission Equipment; (8) Agricultural Machinery and Equipment; (9) New Materials; (10) Biotechnology. The PRC government has issued detailed development plans for each of the ten target industries and it has committed approximately \$300 billion to achieving the plan's objective of transforming China's economic engine from factory-level production to high-technology products and services.

planned to introduce the technology to implement 3-D aircraft design, including 3-D design development environment, design standard based on 3-D modules, 3-D design data module and management, and weight-saving application of 3-D design. The slide had an image which contained the English words, "[Company #1] Digital Metrology Twin Operating Status Monitor." On the "Measurement and Quality Inspection" page, JSL INNOVATIONS highlighted that the PRC relies on foreign software, gives up most of its profits overseas, and that innovation and patent development are controlled by foreign countries. One slide stated that JSL INNOVATIONS wanted to help China make indigenous smart measurement software. One image in the slide matched an image provided in a COMPANY #1 PowerPoint, indicating that LI was referring to the same measurement technology offered by COMPANY #1. The final page contained a graphic showing how the PRC apparently had 2-D technology and JSL INNOVATIONS would help the PRC achieve smart manufacturing.

b. A Word Perfect document dated May 2018, which appears to be a draft letter. The letter is from LI to "G", who, based on the context of the letter, appears to belong to the Shijiazhang government, part of the Hebei Provincial Government. The letter claimed that information attached is JSL INNOVATIONS' technical information and "not to share to the public." In the draft letter, LI provided his itinerary for his trip to Beijing in May 2018 and requested to meet with officials from Shijiazhuang on May 18, 2018.

c. A document with a file name "JSL TechInfo" and titled "Promote Smart Manufacturing Implementation for Chinese Enterprises." The document stated that, "in order to promote 'Made in China 2025' manufacturing plan, Smart manufacturing is more important to China . . . The smart manufacturing . . . can be applied at each processing stage from design, manufacturing, and inspection, to the final product by integrated technologies such as 3-D network visualization of machines and communications, and cloud, big data, some software and hardware." The document further stated that JSL INNOVATIONS was founded in March 2018 and "utilizes expertise from leaders in the field to offer technological consulting with a focus on metrology and smart manufacturing . . . [and] by applying cutting edge technologies . . . JSL Innovations develops the needed software and provides the best solution in short time and low cost to solve the problems. With a team of developers, experts, and marketers, JSL Innovations works on developing beautiful, powerful, and user-friendly solutions customized for the customer's satisfaction." The document offers three services: (1) Smart (mechanical) manufacturing solutions; (2) Enterprise smart manufacturing solutions; and (3) industrial software development. According to the document, these three services, together, would help a company move its product quickly to market. One page included images of COMPANY #1's software and stated that the software is used for digital automation in measurement and quality inspection.

d. Presentations that appeared to be for Beihang University in China, including a PowerPoint presentation dated August 2018 authored by LI. The presentation discussed metrology and stated that "it is even more important in China in order to move forward with the Made in China 2025 manufacturing plan."

e. Presentations that appeared to be for "CNIS," which I believe based on my investigation and my training and experience to refer to the China National Institute of Standardization, which is a division of the PRC government's Standardization Administration. These presentations marketed technology directly related to proprietary technology owned by COMPANY #1 and COMPANY #2.

f. A presentation that appears to be for the Commercial Aircraft Corporation of China ("COMAC"). According to basic Internet research, COMAC is a state-owned enterprise of the PRC government. The presentation discussed COMPANY #1's software and lists specific COMPANY #1 applications.

g. A document dated August 2018, that appears, based on a preliminary translation, to be JSL INNOVATIONS' business plan, with information about founding members. The plan stated that JSL INNOVATIONS provides smart manufacturing and consulting services. The plan stated that JSL INNOVATIONS has its own proprietary software, which it planned to release in early 2019.

h. A document dated July 2019 that appears, based on a preliminary translation, to be a cooperation proposal between JSL INNOVATIONS and PRC EMPLOYER-1. In the proposal, JSL

INNOVATIONS offered its expertise in smart manufacturing, and technology substantially similar to that of COMPANY #1. JSL INNOVATIONS stated that its algorithm code for GD&T software was 80 percent complete.

43. Throughout these and other documents, LI listed his employer as JSL INNOVATIONS and described his background, experience, and capability in technologies related to COMPANY #1 and COMPANY #2 proprietary software.

F. 2018-March 2020: LI Negotiates an Agreement to Conduct a Joint Venture with PRC EMPLOYER-1

44. In or around May 2020, FBI agents recovered from the trash bin on a public street in front of LI's residence what appeared to be pages from an employment agreement between LI and PRC EMPLOYER-1. The agreement was signed by LI and dated March 20, 2020. The agreement set forth a three-year project, for which LI would serve as the chief technical officer. It also stipulated LI could not work less than six months per year in the PRC. The products of the project included overall solutions for smart manufacturing and the development of specific industrial software. The agreement was accompanied by a document stating LI's annual compensation between 2020 and 2023 would be \$170,000.

45. In or around May 2020, FBI agents also uncovered from the trash bin a resume and statement from LI, wherein LI explained his interest in employment in Suzhou, China. According to the document, LI acquired first-hand knowledge of

the PRC's demand for smart manufacturing expertise when he attended international conferences in the PRC. Additionally, while attending two conferences in Beijing in May 2018, he met with H.W., the chairman of PRC EMPLOYER-1, who expressed his desire for LI to work for his firm.

46. Through review of LI's emails, the FBI has identified hundreds of emails from 2018 to 2020 between LI and Chinese entities, including PRC EMPLOYER-1, wherein LI explored business opportunities related to smart manufacturing:

a. Between 2018 and 2020, LI, through his company JSL INNOVATIONS, appeared to engage in several rounds of negotiations with PRC EMPLOYER-1. In December 2018, after months of communication, C.J. from PRC EMPLOYER-1 emailed two documents to J.J. (LI's wife). J.J. forwarded the email to LI. The attachments described a proposed joint venture between PRC EMPLOYER-1 and foreign entity Liming LI, to be based in Suzhou, PRC. The stated goals of the joint venture were to provide technical consulting services for the manufacturing industry, effectively implement smart manufacturing, develop patented industrial software, and enhance smart manufacturing equipment research in the PRC. The company would become a provider of smart manufacturing, MBD/MBE technology, and digital twin solutions, as well as develop its own brand of software products.

b. In or around December 2018, LI engaged a network of consultants based in the PRC with technical backgrounds and business experience to solicit input on the draft agreement from PRC EMPLOYER-1. One associate provided the following feedback:

"If you are satisfied with the valuation of your intellectual property, and the protection of salary during the individual cooperation phase, while avoiding personal financial risk then I think it's a good deal. In 5 years, you can sell your 40%, [PRC EMPLOYER-1] can go on with your intellectual property, it is a win-win situation."

c. In or around March 2019, LI traveled to China to further discuss a joint venture agreement between PRC EMPLOYER-1 and JSL INNOVATIONS. In April 2019, C.J. sent J.J. an amended agreement, based on a conference held in March, which coincided with LI's travel to China. The amended agreement included a third party, Party C. The agreement was also emailed to C.M. Around March 2023, FBI located a LinkedIn profile, written in Mandarin Chinese, which listed C.M. as Chief Secretary for the China Academy of Machinery Science and Technology Group (CAM). Another LinkedIn profile, written in English, listed C.M. as a professor at CAM. According to the publicly-accessible webpage for CAM, viewed by FBI around March 2023, CAM is directly under the leadership of the PRC State-Owned Assets Supervision and Administration of the State Council and is the only PRC state-owned enterprise ("SOE")² engaged in generic and applied technology research and equipment development for the manufacturing industry. Additionally, as of March 2023, the URL "pcmi.com.cn" directs internet users to the homepage for the

² State-owned enterprises are controlled by the State-Owned Assets Supervision and Administration Commission, a PRC government body directly subordinate to the PRC State Council.

Yanqi Lake Basic Manufacturing Technology Research Institute, which, according to its website, is wholly owned by CAM.

d. A few days after the April 2019 email referenced above, C.J. sent a follow-up email, advising the group to reference a new draft agreement which incorporated edits made by C.M. Based on the above information, I believe that PRC EMPLOYER-1 and JSL INNOVATIONS agreed to add a Chinese SOE to their joint venture at their March 2019 meeting and took concrete steps after the meeting to formalize the agreement and establish the venture.

47. In or around March 2020, LI finalized an employment agreement with PRC EMPLOYER-1, in which he agreed to develop technology and intellectual property for PRC EMPLOYER-1 in the field of smart manufacturing. LI exchanged several emails with C.J. and another employee of PRC EMPLOYER-1 about the final employment contract, LI's foreign work permit, and LI's visa application. Much of the technology appeared to be EAR-controlled and trade secret technology related to his work at COMPANY #1 and COMPANY #2, as further described below.

G. September 2020: LI Possesses at his Home Millions of Files Including Proprietary Source Code Belonging to COMPANY #1 and COMPANY #2

48. On September 9, 2020, FBI agents executed a search warrant at LI's residence in Rancho Cucamonga, CA. As detailed below, the items seized included a signed employment agreement between LI and PRC EMPLOYER-1, and digital devices containing millions of files belonging to COMPANY #1 and COMPANY #2, including export-controlled and trade secret source code files, as identified by experts from each of the companies.

49. During the search of LI's residence, FBI agents seized employment documents between PRC EMPLOYER-1 (Party A) and Liming LI (Party B), signed and executed by both parties on or around March 20, 2020. One set of documents was written in English and the other in Chinese characters. According to the English-language version, Party A and Party B agreed to "jointly carry out the projects for developing digitalization of product design, measurement and smart manufacturing technology research and its applications." Party A agreed to pay Party B an annual salary of \$170,000 (before taxes), and the term of the agreement was from March 1, 2020, to approximately February 28, 2023. An annual project bonus would be determined by achievement of the project objectives. The project contents included, among other things, innovation research and development related to smart manufacturing generally, and GD&T and other trade secret technology more specifically.

50. The intellectual property section stipulated that LI agreed to provide all existing intellectual property rights and

technology to PRC EMPLOYER-1. Based on my investigation and my conversations with representatives from COMPANY #1 and COMPANY #2, I am aware that LI owns no patents and has no intellectual property rights in the proprietary source code belonging to COMPANY #1 and COMPANY #2.

51. According to financial records, from around June 2020 to August 2021, LI and J.J. received 15 wire transfers from PRC EMPLOYER-1, totaling approximately \$132,686. Based on my training and experience and knowledge of this investigation, I believe the wire transfers were LI's compensation from PRC EMPLOYER-1 in fulfillment of the above employment agreement. Based on my review of records and conversations with COMPANY #2 representatives, I believe that LI never disclosed his employment with PRC EMPLOYER-1 to COMPANY #2, even though LI was actively negotiating the terms of his employment with PRC EMPLOYER-1 while he was still employed by COMPANY #2.

52. In September 2020, after the execution of the search warrant at his residence, FBI agents interviewed LI. According to the transcript of the recorded interview, LI confirmed he provided consulting services to China-based companies. LI initially stated he did not possess any source code files from his previous employers and maintained that his consulting services were conducted lawfully. Later in the interview, LI stated it was possible some of his devices contained proprietary source code. Then, later in the same interview, LI admitted some of his devices contained proprietary source code, and he referenced that source code when building his own software. LI

further admitted that his representation to PRC EMPLOYER-1 that his own GD&T software was 80 percent complete was a lie. In fact, as detailed below, LI possessed numerous digital devices containing millions of files related to the work of COMPANY #1 and COMPANY #2, including proprietary source code files.

53. Specifically, agents have identified millions of files, including reference guides, promotional materials, and thousands of proprietary source code files belonging to COMPANY #1 and COMPANY #2, which were stored across multiple of LI's digital devices, including computers and hard drives. Many of those proprietary source code files were stored within folders containing labels such as JSL and JSL Projects and were clearly identified by COMPANY #1 and COMPANY #2 header information. COMPANY #1 subject matter experts have also identified on LI's devices some proprietary source code files belonging to COMPANY #1 that appear to have been superficially modified by LI to include JSL, rather than COMPANY #1, in the header information.

54. Among other things, these source code files pertained to six key aspects of COMPANY #1's proprietary software suite, including Geometric Dimensioning and Tolerancing ("GD&T"), airfoil inspection, Measuring Pathways, CAD software used to operate a REVO Probe, Collision Detection, and Best Fit calculations, as described below:

a. GD&T is a system used by engineers to communicate how accurately a part must be manufactured to meet a particular industry standard.

b. Airfoil inspection is the measurement and analysis of curved structures, such as aircraft turbine blades, which require special calculations.

c. Measuring Pathways describes the movement of a probe by a CMM to measure a workpiece accurately and efficiently.

d. A REVO Probe is an instrument used by a CMM to scan and measure a workpiece.

e. Collision Detection prevents unintentional contact between machines, measuring instruments, and workpieces.

f. Best fit calculations determine the location and direction of a workpiece and reconcile measurement data with design data and can be used in the absence of an industry standard.

55. FBI interviewed subject matter experts at COMPANY #1 on multiple occasions, including August 2022 and April 2023. FBI also interviewed subject matter experts at COMPANY #2 in July 2022. According to the reports of their interviews, the subject matter experts confirmed that many of the proprietary source code files found on LI's devices in fact constituted trade secrets belonging to COMPANY #1 and COMPANY #2, respectively. The COMPANY #1 expert, M.S., also stated that the naming convention on many of the trade secret files made clear that the files contained proprietary source code, and that it would be very unlikely for someone in LI's possession to integrate such code into his own software by accident.

56. According to the reports of the interviews of COMPANY #1 and COMPANY #2 experts, both COMPANY #1 and COMPANY #2 had

taken steps to protect their trade secret proprietary source code files, including:

- a. Limiting physical access to the locations within the company where the trade secrets were stored using keys, key cards, and key codes;
- b. Limiting access to the trade secrets only to those who possess company network credentials and require access to the trade secrets to perform their employment duties;
- c. Requiring employees to sign nondisclosure and confidentiality agreements that prohibited disclosure of trade secrets and confidential and proprietary information and extended beyond the term of employment;
- d. Mandating visitor sign-in sheets, escorts, and non-disclosure agreements; and
- e. Providing training and instruction regarding the security and safeguarding of restricted and confidential business information.

57. According to FBI interview reports, COMPANY #1 and COMPANY #2 management indicated that LI's possession of their source code files on his personal devices would violate their respective company policies, including policies on which LI was specifically trained and which LI signed. Executives from COMPANY #1 and COMPANY #2 also stated to the FBI that they derived significant economic value from the secrecy of their source code files, including the specific files that LI possessed, as detailed below. Executives from both companies

stated that the companies would likely incur significant financial damage if the files were disseminated to competitors.

H. March-May 2020: LI Attempts to Travel to China

58. As noted above, according to the executed employment agreement, LI was required to spend at least six months per year in China in support of his joint project with PRC EMPLOYER-1. Based on my review of LI's email account, in March 2020, PRC EMPLOYER-1 sent LI a plane ticket on China Airlines flight CI 23, departing from Ontario International Airport and arriving in Taipei, Taiwan. From Taipei, LI was scheduled to continue on to Shanghai, China, on another China Airlines flight. Due to travel restrictions related to the COVID-19 pandemic, however, LI was unable to travel to China at the time.

59. Based on my review of LI's email account, around March 2020, LI sent an email to a general account for the People's Republic of China Consulate General for Los Angeles (PRCCONLA). The email included an attachment named "Liming_Material For Chinese Visa" [sic], in which LI explained he had been hired by PRC EMPLOYER-1 as Chief Technologist to conduct smart manufacturing research and application. LI planned to fly to China in March but learned there was a pause on foreigner travel to China, so he was writing to submit another visa request. The attachment also included photos of LI's U.S. passport, Chinese visa, signed and stamped employment agreement with PRC EMPLOYER-1, contact information for C.J., original flight itinerary, and quarantining instructions from the City of Suzhou. In or around March 2020, C.J., on behalf of PRC EMPLOYER-1, helped LI obtain

a work permit. Shortly thereafter, LI emailed PRCCONLA a Chinese work permit issued by the National Foreign Expert Bureau.

60. Based on my review of LI's email account in or around May 2020, LI emailed PRCCONLA, including a letter attachment from PRC EMPLOYER-1, dated May 12, 2020. The letter was addressed to LI, thanking him for accepting the employment offer with PRC EMPLOYER-1 and urging him to report to China before March 1, 2020, to participate in the smart manufacturing project. It further stated the project was important to the improvement of small- and medium-sized manufacturing enterprises as well as the local government's industrial information sector. The project had already passed review by the local government, and LI was required to participate in a technology question and answer (Q&A) session after a site survey. The letter urged LI to come to China as soon as possible because his attendance would affect the progress of the project. C.J. was listed as the point of contact.

61. Around May 12, 2020, LI sent another email to PRCCONLA, which emphasized that LI intended to return to China to guide a smart manufacturing project, and it was a key moment for the industry of smart manufacturing. He also urged PRCCONLA to consider China's policy priority to import key foreign technology. LI also stated he had quarantined at home for the past two months. LI appeared to receive an automated email in response.

62. Around May 19, 2020, LI forwarded C.J. an email regarding HOOPS virtual training. The forwarded email described HOOPS as a web platform enabling users to import and visualize computer-aided design (CAD) program. LI asked C.J. to forward the email to the software team at PRC EMPLOYER-1.

63. Based on the above communications, as well as the 15 wire payments received by LI from PRC EMPLOYER-1 starting in June 2020, I believe that LI and PRC EMPLOYER-1 initiated the smart manufacturing project, despite global circumstances preventing LI from traveling to China at the time.

I. February-May 2023: LI Travels to Taiwan

64. According to travel records, on or around February 18, 2023, LI flew to Taipei, Taiwan from Ontario, CA, on the exact same China Airlines flight (CI 23) that PRC EMPLOYER-1 had purchased for LI in March 2020. Although LI has flown internationally from the United States more than 40 times between 2005 and 2020, he had never flown to Taiwan before his February 2023 departure. While LI has flown directly from the United States to China in the past, I know from my training and experience that individuals engaged in unlawful activity often attempt to conceal their travel and whereabouts from law enforcement detection.

65. I also know individuals engaged in unlawful activity are aware that U.S. law enforcement keep inbound and outbound travel records, but U.S. law enforcement may not be able to monitor an individual's travel between two non-U.S. countries with the same astuteness. As a result, individuals engaged in

unlawful activity may obscure their international travel by flying to one country first and booking travel to their intended final destination after their arrival, masking their intended destination from the U.S. government. In some circumstances, these individuals may travel using a different travel document than the one used when they departed the United States to further evade detection.

66. According to travel records, on or around April 6, 2023, LI was scheduled to depart Taipei, Taiwan and arrive in Ontario, California on China Airlines (CI24). However, LI was not on board. Updated records reveal that LI is currently scheduled to return to the United States on May 6, 2023.

67. Based on the matching flight, LI's past travel, and my knowledge of strategies used by criminals to thwart law enforcement detection, I believe LI likely traveled to China in February 2023 and took measures to obscure this information from the U.S. government.

68. On April 4, 2023, the FBI obtained a warrant to search the person of LI, but that warrant was never executed because LI missed his April 6, 2023, return flight.

69. According to email records, LI received approximately 13 emails from PRC EMPLOYER-1 employee C.F., between April 18 and April 20, 2023. By contrast, between March 27 and April 17, 2023, C.F. had sent just one email to LI.

70. Based on LI's extensive prior communications with PRC EMPLOYER-1, his travel on the same itinerary that PRC EMPLOYER-1 previously purchased for him in 2020, and his sudden increase in

email communications with PRC EMPLOYER-1 employee C.F., as well as my knowledge of this investigation and my training and experience, I believe LI's present travel to China was likely to promote LI's work with PRC EMPLOYER-1, which includes his attempts to use the trade secrets he stole from COMPANY #1 and COMPANY #2 to help PRC EMPLOYER-1 develop its smart manufacturing capabilities.

71. Based on my knowledge of this investigation and my training and experience, I believe that evidence relating to LI's travel, including meetings with PRC EMPLOYER-1 and/or other Chinese entities or state-owned enterprises, and efforts to use the stolen trade secrets to support those entities, is likely to be found on LI's digital devices. Specifically, I believe LI likely uses WeChat to communicate with entities in China. Based on my knowledge, training, and experience, I know WeChat is the dominant messaging application in China.³ The platform also integrates telecommunications, social media, retail, and other functions into a single platform, and is headquartered in China. Based on my law enforcement training and experience, I know WeChat is not responsive to U.S. legal process. As a result, individuals conducting unlawful activity may conceal their communications from U.S. law enforcement entities by utilizing

³ Records provided by T-Mobile for LI's cell phone, which were current as of approximately April 4, 2023, did not show any phone calls between LI and accounts in the PRC. Based on my training and experience, I know that WeChat communications would not show up on such records.

WeChat for voice calling, messaging, financial transactions, and other functions.

72. During this investigation, FBI agents identified screen captures from LI's mobile device, which LI forwarded to himself in emails and saved on other digital devices. Specifically, in March 2020, LI emailed himself a screenshot of what appeared to be a conversation between C.J. and LI over WeChat, wherein C.J. provided LI with information regarding LI's upcoming trip to China. LI indicated "she" (likely J.J.) would call C.J. regarding the ticket purchase.

73. FBI agents also uncovered an August 2018 email between Z.J., a human resources representative for COMAC (as noted above, a state-owned enterprise of the PRC government) and LI. Z.J. wrote that Z.J. had received LI's resume and instructed LI to call Z.J. using WeChat. Based on a review of LI's Thousand Talents Plan application, LI received letters of recommendation from COMAC staff regarding his participation in the Thousand Talents Plan around that time.

74. For these reasons, I submit that there is probable cause that any digital device contained on LI's person upon his return travel will contain evidence of the SUBJECT OFFENSES.

VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES⁴

75. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I

⁴ As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units;

know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable

desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

76. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which

may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

77. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when

a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress LI's thumb and/or fingers on the device(s); and (2) hold the device(s) in front of LI's face with his eyes open to activate the facial-, iris-, and/or retina-recognition feature.

VII. REQUEST FOR NIGHT SERVICE

78. I request that the search of LI's person be authorized at any hour of the day or night. FBI agents intend to execute the search upon LI's arrival on an inbound international flight. Because unexpected delays may arise that are outside the control of the government, including airline delays and delays in disembarking and travel through customs and immigration processes, there is a significant possibility that the FBI may be unable to execute the warrant until after 10:00 P.M.

VIII. CONCLUSION

79. Based on the foregoing, there is probable cause to believe that LI has committed a violation of 18 U.S.C. § 1832: Theft of Trade Secrets. There is also probable cause that the

items to be seized described in Attachment B will be found in a search of LI's person, as described in Attachment A.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this ____ day of _____, 2023.

HONORABLE MARIA A. AUDERO
UNITED STATES MAGISTRATE JUDGE